IN UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, *et. al* Plaintiffs, v. BARACK HUSSEIN OBAMA II, *et. al* Defendants.	Civil Action No. 13-CV-851

LARRY KLAYMAN, *et. al* Plaintiffs, v. BARACK HUSSEIN OBAMA II, *et. al* Defendants.	Civil Action No. 13-CV-881

PLAINTIFFS' REPLY IN SUPPORT OF THEIR MOTIONS FOR PRELIMINARY INJUNCTION

I. INTRODUCTION

"Freedom is never more than one generation away from extinction. We didn't pass it to our children in the bloodstream. It must be fought for, protected, and handed on for them to do the same." - President Ronald Reagan

The National Security Agency ("NSA") has been collecting mass amounts of telephony and metadata in violation of the Patriot Act and the First, Fourth, and Fifth Amendments to the U.S. Constitution. Despite the NSA's false arguments to the contrary, none of the Defendants' actions are condoned under U.S. law, and the NSA has been acting in violation of the law for as long as the NSA and PRISM data collection programs have been ongoing.

The NSA has shown a pattern of lying to the American people, including by James Clapper, the Director of National Intelligence. In addition, the Obama administration has been caught lying in one scandal after another, including but not limited to Obamacare, Benghazi, the IRS, and Fast and Furious, just to name a few.

It was not until the actions of key NSA whistleblower Edward Snowden that the American people became aware of the illegal actions their own government was taking against them. Plaintiffs filed two lawsuits, the first challenging the constitutionality of the NSA's actions in collecting telephony metadata from Verizon as a result of secret Foreign Intelligence Surveillance Act court ("FISC") orders.

Subsequently, Plaintiffs' second lawsuit challenged the warrantless searches of the NSA's PRISM program[1], which would monitor and intercept communications from internet companies such as Skype, Google, Youtube, AOL, Yahoo!, Facebook, Paltalk, AT&T, Sprint, and Microsoft. In collaboration with these internet companies, PRISM allows the NSA to directly access and retrieve private electronic data belonging to all users and customers of Defendants' online services. As Snowden revealed, he, sitting at his desk, could "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email." Glen Greenwald, "*XKeyscore: NSA tool collects 'nearly everything a user does on the internet*'," The Guardian (July 31, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. Even more outrageous, programs such as these *were* used to illegally wiretap Chancellor Angela Merkel of Germany. *See* Alison Smale and David E. Sanger, "*Spying Scandal Alters U.S. Ties With Allies and Raises Talk of Policy Shift*," The New York Times (November 11, 2013), http://www.nytimes.com/2013/11/12/world/spying-scandal-alters-us-ties-

[1] The PRISM program did not receive a court order from the FISC.

with-allies-and-raises-talk-of-policy-shift.html. The NSA has previously stated that programs such as these are required to ensure that terrorist organizations and located and stopped. Yet it is inconceivable that the wiretapping of Chancellor Merkel is related to the tracing of terrorist activities.

PRISM far exceeds statutory and constitutional authority, requiring no level of reasonable suspicion or probable cause while incredibly given the NSA direct and unfettered access to some of the largest databases in the world maintained by the NSA. The NSA has direct access to records detailing the daily activities, interactions, social, political, and personal associations, as well as private and intimate facts of millions of ordinary Americans.

Plaintiffs believed that as the truth was exposed that the government would cease performing these illegal actions. Yet as time went on, it became evident that the NSA was continuing with these secret programs, and in fact even more secret actions were exposed. New evidence had come to light every week demonstrating more and more violations by the NSA of the Plaintiffs rights. For this reason, Plaintiffs realized that a preliminary injunction would be necessary to ensure that no further illegal actions would be taken by the NSA.

In their opposition to Plaintiffs' Motion for Preliminary Injunction, the NSA characterized their massive data collection scheme as a lawful, effective counter-terrorism mechanism, closely monitored and safeguarded to ensure that the American people's rights are fully protected. Nothing could be further from the truth. From the actions of one key whistleblower, Edward Snowden, the American people have realized that the NSA is engaging in Orwellian surveillance that is simultaneously collecting data on hundreds of millions of phone and internet users.

Plaintiffs, and this Court, cannot rely on the statements made by the NSA in their pleadings. All the evidence shows that the NSA has been acting in clear violation of the Patriot Act and the U.S. Constitution. Even if the Court were to accept the Defendants' affidavits, then the parties must go to discovery. The Plaintiffs have more than demonstrated the need for a preliminary injunction to be granted against the NSA's unlawful and unconstitutional actions. Plaintiffs are more than likely to succeed on the merits of this lawsuit, and the irreparable injury occurring toward the Plaintiffs in this lawsuit will continue for as long as this data collection program is allowed to act outside of the law.

Plaintiffs simply seek to have the NSA enjoined into following the law. Nothing more. A preliminary injunction, and a subsequent permanent injunction, are needed to ensure that the NSA discontinues acting in violation of the Patriot Act and the U.S. Constitution and nothing that the NSA has presented has in any way demonstrated that it has been acting in the scope of the law. The Court must respectfully similarly construct an oversight mechanism to ensure that the NSA is following the law. Without this injunctive relief, the NSA will continue to collect massive amounts of private information from hundreds of millions of the American people, in the largest violation of Patriot Act and the U.S. Constitution in history.

II. THE LAW

A. THIS COURT HAS JURISDICTION TO HEAR THIS CASE

The U.S. Constitution directly vests the District Court with original jurisdiction to hear this case. Article III, Section 2, states that "[t]he judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution..." U.S. Const. Art. III, Sec. 2.

Jurisdiction is also proper under 28 USC § 1331, which states that, "[t]he district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States." 28 USC § 1331. See also *Sanders v. Murdter*, 516 Fed. Appx. 4, 5 (D.C. Cir. 2013) ("Appellant is correct that the district court had federal-question jurisdiction over his claims arising under the Constitution") citing 28 USC § 1331; *Bell v. Hood*, 327 U.S. 678, 66 S. Ct. 773, 90 L. Ed. 939 (1946).

Here, Plaintiffs' claims are arising directly out of the Patriot Act and the First, Fourth, and Fifth Amendments to U.S. Constitution, and this Court has original jurisdiction pursuant to the U.S. Constitution and 28 USC § 1331.

B. A PRELIMINARY INJUNCTION IS PROPER

To obtain injunctive relief, Plaintiffs must only demonstrate (1) a substantial likelihood of success on the merits; (2) that they are likely to suffer "irreparable injury" if preliminary relief is not granted; (3) that an order would not substantially injure other interested parties; and (4) that the public interest would be furthered by granting the order. *Washington Metro. Area Transit Comm'n v. Holiday Tours, Inc.*, 559 F.2d 841, 843 (D.C. Cir. 1977); *Citigroup Global Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 35 (2d Cir. 2010). These four factors must be viewed as a continuum where greater strength in one factor compensates for less in the other: "If the arguments for one factor are particularly strong, in injunction may issue even if the arguments in other areas are rather weak." *CityFed Financial Corp. v. Office of Thrift Supervision*, 58 F.3d 739, 747 (D.C. Cir. 1995).

a. Plaintiff's Have Demonstrated A Likelihood Of Success On The Merits

1. The NSA's Collection of Metadata is Not Authorized Under 215 of the Patriot Act

In its current form, Section 215 allows the NSA to obtain an order compelling production of "any tangible things" upon a "showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation…to obtain foreign intelligence information not concerning United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. §1861(b)(2)(A).

Section 215 of the Patriot Act does not provide the NSA with limitless investigative power. Rather, the language added by the Patriot Act prohibits the government from using the statute to obtain things that could not be obtained through analogous mechanisms, such as a subpoena duces tecum. *Id*. §1861(c)(2)(D).

Defendants' unlawful surveillance further exceeds the authority provided under Section 215 because it involves surveillance that is *prospective* rather than retrospective. Section 215 permits the government to collect already-existing records, ***not*** to engage in ***ongoing*** surveillance. *See* 50 U.S.C. 1861(c)(1)-(2) (contemplating the "release" of tangible things" that can be "fairly identified" after a "reasonable period of time within which the tangible things can be assembled and made available."). The Verizon Order requiring Verizon to provide the NSA access to extensive and voluminous communication records on an "***ongoing daily basis***" is an ongoing production obligation—an obligation that is effectively indefinite. This is clearly contrary to the language of the statute and cannot be reconciled with the plain language of Section 215 of the Patriot Act. Defendants have undeniably exceeded the bounds of their statutory and constitutional authority, and the Verizon Order, which ordered the ongoing production of prospective communication records, and thus is contrary to the plaintiff language of Section 215, clearly went far beyond the limitations set out in the Patriot Act.

Defendants "secret interpretation" of Section 215 (or, more appropriately, absolute disregard of the limitations set forth in Section 215) has been evidenced through numerous instances of unlawful conduct, including repeatedly misleading the FISC, presenting inaccurate statements in court filings, making false misrepresentations, and exceeding the bounds of the surveillance as set forth in court orders. *See* Nicole Perlott, Jeff Larson, and Scott Shane, *"N.S.A. Able to Foil Basic Safeguards of Privacy on Web,*" The New York Times (Sept. 5, 2013) http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html. Even more outrageous is the number of misleading statements senior officials have made about domestic surveillance and the extent of the NSA's false misrepresentations and blatant lies. These officials have engaged in obstruction of justice, with impunity. The National Intelligence Director, James Clapper, testified before Congress earlier this year that the NSA does not collect data on millions of Americans, which he now admits is a "clearly erroneous" lie. Clapper was asked during a hearing in March by Sen. Ron Wyden if the NSA gathered "any type at all on millions or hundreds of millions of Americans."[2] Clapper initially answered definitely: "No." When pressed by Widen, Clapper changed his answer. "Not wittingly," he said. "There are cases where they could inadvertently perhaps collect, but not wittingly." Nothing could be further from the truth, as evidenced by the public disclosures of a highly classified "Verizon Order" in addition to Clapper subsequently apologizing for, and thus admitted, his clearly erroneous and untruthful answer.

The NSA's use of the PRISM program is an entirely different matter. Rather than limit its surveillance to a certain group of people that are subjects of an authorized investigation, the

[2] *See*, "*Clapper apologizes for 'erroneous' answer on NSA*." http://news.yahoo.com/clapper-apologizes-erroneous-answer-nsa-221238030.html (summarizing Clapper's misleading statements to Congress on the extent of U.S. surveillance on U.S. citizens).

government has instead, *without a warrant*, collected and stored "metadata" of hundreds of millions of U.S. citizen internet users, regardless of whether or not they are persons of interest. It is simply inconceivable to conclude that ***all*** communication records and internet activities records for ***all*** customers of the major internet companies involved bear some relevance to an investigation, nor is there any reasonable grounds to believe that they may be relevant to an authorized investigation, in any conventional sense of that phrase. To the contrary, the vast majority of the communication records obtained through the broad sweeping surveillance are, in fact, not relevant to any authorized investigation. The government has not, and cannot, demonstrate, through specific and articulable facts, that the indiscriminate, unfettered, bulk collection of hundreds of millions of Americans' internet records was a warranted and justified intrusion on privacy rights.

Despite the NSA's repeated false allegations about the safeguards put in place to protect the privacy of Americans, NSA personnel have been blatantly misusing the NSA's surveillance power to spy on their paramours. NSA Inspector General George Ellard admitted that since 2003, there have been "12 substantiated instances of intentional misuse" of "surveillance authorities." See Exhibit 1 -- Letter of NSA Inspector General George Ellard to Senator Chuck Grassley. About all of these cases involved an NSA employee spying on a girlfriend, boyfriend, or some kind of love interests. Jake Gibson, *"Too tempting? NSA watchdog details how officials spied on love interests,"* FOX News, (Sept. 27, 2013). http://www.foxnews.com/politics/2013/09/27/too-tempting-nsa-details-how-officials-spied-on-love-interests/.

Courts consider a threat to attorney-client communications an exceptional circumstance and have issued writs of mandamus to vacate production orders implicating privileged

information. See, *e.g., In re BankAmerica Corp. Sec. Litig.*, 270 F.3d 639 (8th Cir. 2001) (attorney-client); *Admiral Ins. Co. v. U.S. Dist. Court for the Dist. of Ariz.*, 881 F.2d 1486 (9th Cir. 1989) (attorney-client); *In re Fink*, 876 F.2d 84 (11th Cir. 1989) (doctor-patient). In this case, the FISC issued a blanket order for all domestic telephone records. Such a boundless order sweeps up not just communications protected by attorney-client privilege, but also those falling under marital communications privilege, psychiatrist-patient, privilege, accountant-client privilege, and clergy-pertinent privilege.

The FISC does nothing more than rubber stamp the applications of the FBI. These proceedings offer nothing more than one sided arguments from those seeking the warrants. There are no adversaries to present alternative arguments, and innocent Americans have no advocate to argue against these widespread, illegal searches. The secrecy of the FISC court, and the limited number of personnel working within it, has created an incestuous atmosphere and not an adversarial proceeding in which the rights of the innocent are protected.

Furthermore, the FISC court has made findings of repeated violations of court orders. In 2011, the Honorable John D. Bates, then serving as chief judge on the FISC, admonished the NSA for repeatedly violating the requirements and limitations set forth by Court Orders, privacy laws, and the U.S. Constitution. As Judge Bates emphasized, "[c]ontrary to the government's repeated assurances, N.S.A. has been routinely running queries of the metadata using querying terms that did not meet the standard for querying," and that this requirement had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall…regime has never functioned effectively." Charlie Savage and Scott Shane, *"Secret Court Rebuked N.S.A. on Surveillance*," The New York Times, (Aug. 21, 2013).

http://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html?r=0.

Judge Bates further emphasized the NSA's unlawful conduct and egregious and illicit surveillance tactics, by stating:

> "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program. In March, 2009, the Court concluded that it s authorization of NSA's bulk acquisition of telephone call detail records from [redacted] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his 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…"

Memorandum Opinion, *In re Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certification* (FISC Ct. Oct. 3. 2013) at fn. 14.

The NSA has continuously engaged in a pattern of non-compliance with respect to the NSA's handling of produced information, as demonstrated through publicly released FISC orders addressing the NSA's surveillance and requests for production of information. In her Amended Memorandum Opinion, dated August 29, 2013, the Honorable Claire V. Eagan recognized and acknowledged Defendants' repeated lack of adherence to minimization procedures implicit in the authorization to compel production of the documents, stating, "[t]he Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information." Amended Memorandum Opinion, *In Re Application of the Federal Bureau of Investigation For An Order Requiring the Production Of Tangible Things From [Redacted]*, (FISC Ct. Aug. 29, 2013) at n.9.

Similarly, in an order issued by the FISC on March 2, 2013, questioning the credibility, trustworthiness, and ability for the NSA to fully comply with court orders, the Honorable Reggie B. Walton held, "[i]n light of the scale of this bulk [telephone records] collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified…and that it is being implemented in a manner that protects the privacy interests of U.S. persons as required by applicable minimization procedures. To approve such a program, the Court must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders. ***The Court no longer has such confidence***." [emphasis added] *In Re Production of Tangible Things [Redacted]*, Dkt. No: BR. 08-13 (FISA Ct. March 2, 2009).

The actions of the NSA went beyond scope of the Patriot Act, and as such these actions are unconstitutional as violations of the First, Fourth, and Fifth Amendments to the U.S. Constitution.

2. Plaintiffs Have Demonstrated a Fourth Amendment Violation

The NSA's PRISM surveillance program consists of warrantless searches, which "are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967); *see United States v. Karo*, 468 U.S. 705, 717 (1984). In fact, it authorizes the particular form of search that the authors of the Fourth Amendment found most offensive, leaving "too much to the discretion of the officer executing the order." *Berger v. New York*, 388 U.S. 41, 59 (1967). Even if the warrant requirement does not apply, the government's over broad, dragnet collection of Plaintiffs' phone records and internet activities is unreasonable and, therefore, unconstitutional.

"[T]he ultimate touchstone of the Fourth Amendment" is "reasonableness." *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). Reasonableness is determined by examining the "totality of circumstances" to "assess, on the one hand, the degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006); *see also Virginia v. Moore*, 553 U.S. 164, 169 (2008). In the context of electronic surveillance, reasonableness demands that statues have "precise and discriminate" requirements and that the government's surveillance authority be "carefully circumscribed so as to prevent unauthorized invasions of privacy." *Berger*, 388 U.S. at 58.

The data obtained by the NSA through PRISM, done so without any court order, not only includes the contents of emails, chats, VoIP calls, and cloud-stored files, and more but also provides the Agency with online metadata, such as email logs, geolocation data (IP addresses), and web search activities, which can be just as revealing as the content. The NSA is using the troves of metadata gathered by PRISM to build comprehensive profiles of ordinary Americans, including their social connections, familial, political, professional, religious, and personal associations, speech, location, and public movements, while revealing personal, intimate, and, often times, extremely sensitive details about an individual.

Indeed, the NSA's collection of metadata and surveillance of telephonic communications lacks any indicia of reasonableness, as it significantly invades Plaintiffs' privacy rights without any probable cause or individualized suspicion, is essentially indefinite, lacks any measure of particularity, instead gathering vast quantities of information about essentially every individual's communication and activities. In fact, NSA's warrantless surveillance is so extreme in its intrusive nature that it can hardly be construed as anything but unreasonable.

In addition, the Verizon Order requires the production of every communication record, with no attempt to narrow the records obtained to those records that pertain to an ongoing investigation or that have some indication of suspicious activity. The Verizon Order does not differentiate between individuals that the NSA has a legitimate interest in monitoring and those that it does not, nor does it draw a distinction between those records relevant to an investigation and those that are not.

The NSA's opposition to Plaintiffs' Fourth Amendment claim relies heavily on *Smith v*. *Maryland*, 442 U.S. 735 (1979). The NSA, however, fail to recognize that *Smith* does not stand for the proposition that the Constitution permits the indefinite collection of sensitive information about every single phone call made or received by U.S. residents In *Smith*, the Supreme Court upheld the installation of a "pen register" in a criminal investigation. The pen register in *Smith*, however, was very primitive—it tracked the numbers being dialed, but it did not indicate which calls were completed, let alone the duration of those calls. 442 U.S. at 741. It was in place for less than two days, and it was directed at a single criminal suspect. *Id*. at 737.

PRISM provides the NSA with direct access to all private electronic data belonging to all users of the internet services, with no attempt to narrow the records obtained to those records that pertain to an ongoing investigation or that have some indication of suspicious activity. The PRISM program does not differentiate between individuals that the NSA has a legitimate interest in monitoring and those that it does not, nor does it draw a distinction between those records relevant to an investigation and those that are not.

The PRISM program is essentially indefinite, particularly considering the lack of any temporal limitation and the fact that it has been ongoing, secretively, for the past seven years. PRISM provides the NSA with access to and potential production of online communication

records on an ongoing daily basis, with absolutely no temporal deadline or any indication of when the program will terminate. To the contrary, the NSA apparently intends to continue the surveillance program indefinitely, and pursue the ongoing production of communication records of hundreds of millions of Americans for the foreseeable future.

With the Verizon order, the NSA seeks to track the records of millions of Americans, the vast majority of whom are not involved with any terrorist activities. Unlike in *Smith*, where the information from the pen register was not aggregated with information from other pen registers, telephony metadata encompasses far more than just the simple call records. As alleged by Plaintiffs, "Telephony metadata includes comprehensive communications routing information, including, but not limited to, session identifying information (e.g. originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifiers, telephone calling card numbers, and time and duration of call." Compl. ¶¶27, 28. All this information goes beyond just a pen register. And can be easily used to track a person's name and identity. Further, the "call detail records" referred to in the Verizon Order likely include "[a]ny information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of any call." 47 C.F.R. §64.2003 (2012) (defining "call detail information"). Even more absurd, the NSA seeks to collect this information on an ongoing basis. The NSA cannot hide behind *Smith* and claim every one of its actions are legal under this one precedent, because their actions go far beyond what the U.S. Supreme Court allowed in *Smith*.

The NSA also contends, again citing *Smith*, that individuals lack a constitutionally protected privacy interest in telephony metadata because that information has been shared with telephone companies. But the NSA's reading of *Smith* fails to account for *Jones* and a host of Supreme Court cases recognizing that in sharing information with the public or a third party, individuals do not necessarily surrender their expectation of privacy. *See United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *Id.* at 964 (Alito, J., concurring); *see also, e.g.*, *Florida v. Jardines*, 133 S. Ct. 1409 (2013) (odors detectable by a police dog that emanate outside of a home); *Kyllo*, 533 U.S. 27 (thermal signatures emanating from a home); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (diagnostic-test results held by hospital staff). These cases confirm that an individual's expectation of privacy in information does not hinge simply on whether she has shared it with another person. Were it otherwise, even the *contents* of one's phone calls or email would be constitutionally unprotected, as both are shared with third parties. To contend that *Smith* controls here is to misunderstand the narrowness of the pen register surveillance upheld in that case, the breadth of the surveillance at issue here, or both.

3. Plaintiffs Have Demonstrated a First Amendment Violation.

The Supreme Court has recognized the profound chilling effect of government surveillance on First Amendment rights, given their potential to stifle free association and expression. As stated most recently in *United States v. Jones,* "awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." *United States v. Jones*, 132 S. Ct. 945, 956 (2012). Thus, the courts have subjected such investigative methods to "exacting scrutiny" where they substantially burden First Amendment

Rights. *In re Grand Jury Proceedings*, 776 F.2d 1099, 1102-03 (2d Cir. 1984); *Clark v. Library of Cong.*, 750 F. 2d 89, 94 (D.C. Cir. 1984). Under this demanding standard, the NSA is required to show that its investigative methods are the least restrictive means of pursuing a compelling state interest. *Clark*, 750 F.2d at 95. "This type of scrutiny is necessary even if any deterrent effect on the exercise of First Amendment right arises, not through direct government action, but indirectly as an unintended but inevitable result of the government's conduct," *Elrod v. Burns*, 427 U.S. 346, 362 (1976) (quoting *Buckley v. Valeo*, 424 U.S. 1, 65 (1976); see also *Bates v. City of Little Rock*, 361 U.S. 516, 523 (1960) ("Freedoms such as these are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference.")

The Supreme Court has frequently emphasized the importance of preserving the First Amendment rights of advocacy groups, recognizing that the NSA'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 *N.A.A.C.P. v. Button*, 371 U.S. 415, 433 (1963). In *NAACP v. Alabama ex rel. Patterson*, 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." 357 U.S. 449, 462 (1958).

As discussed above, the NSA's broad sweeping surveillance program, in both the telephony metadata collection and the PRISM program's data collection, raises precisely the same associational harm, since Plaintiffs are particularly vulnerable to this type of surveillance and the information collected, given their professions, political activism, public personas, and their activities, which often involve highly confidential matters and privileged information. Under PRISM, the NSA has direct access to records detailing the daily activities, interactions, social, political, and personal associations, as well as private and intimate facts of millions of ordinary Americans.

Further, the mass surveillance program and the broad-sweeping Verizon Order exposes private and sensitive information regarding Plaintiffs' communications and contacts, which consequently directly impacts their ability to continue their advocacy activities.

In light of his public advocacy in matters of public interests and concern, Plaintiff Klayman 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 communicates with these individuals, who may ultimately become clients, regarding potential legal representation and bringing a legal action to redress their harm. Plaintiff Klayman also regularly engages in telephone calls with clients he is already representing, where he discusses legal matters and advises the client, 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 their inherent affects on government policy and acts, Plaintiffs' communication records contain confidential and even legally-privileged discussions that were never intended to be collected, monitored, or heard and recorded by the NSA, particularly as Plaintiffs' advocacy often espouse dissident beliefs than that of the Obama administration.

All of these individuals, particularly those who seek legal advice from Plaintiff Klayman, have an interest in maintaining the confidentially of their communications, and all of these individuals contribute significantly to Plaintiffs' First Amendment activities. It is indisputable that any person would be hesitant to approach Plaintiffs in regard to their advocacy or legal representation, particularly with the knowledge that the NSA receives and records every telephone call through this surveillance program. Thus, the NSA's mass call-tracking surveillance program has inevitable had a chilling effect, as it allows the government to uncover anonymous tips or attempts by individuals to privately share sensitive information with Plaintiffs. Consequently, the governments' surveillance program is directly inhibiting and deterring crucial sources of information for Plaintiffs' work.

4. Plaintiffs Have Demonstrated a Fifth Amendment Claim.

Plaintiffs have an individual privacy interests in their internet communications online activities, which reveals sensitive, confidential information about their personal, political, and religious activities and which Plaintiffs do not ordinarily disclose to the public or to the government. This privacy interest, particularly in their communications, is protected by numerous state and federal laws well as the substantive and procedural right to due process under the Fifth Amendment.

Plaintiffs' Fifth Amendment constitutional rights were clearly violated the moment Defendants provided and the NSA obtained direct and unlimited access and authority to obtain vast quantities of communication records contained in Defendants' vast databases, which inherently includes communication records belong to Plaintiffs. Under PRISM, Defendants have illicitly provided the NSA with blanket access to their vast databases, allowing the NSA to secretively collect, acquire, retain, search, and use the bulk private internet data and online communication information of Plaintiffs, without providing any notice to Plaintiffs, or any process by which Plaintiffs could seek redress. Moreover, the NSA's surveillance was conducted without any individualized suspicion, probable cause, or other governmental interest sufficient or narrowly tailored to justify the invasion of Plaintiffs' due process rights. Prior to *The Guardian's* and *The Washington Times* publication of the disclosures of NSA whistleblower, Edward Snowden, this secret surveillance was undisclosed to the public, and Plaintiffs had no notice and no reasonable opportunity to discover the existence of the surveillance program, let alone ascertain where a reasonable expectation of privacy from government intrusion begins and ends and specifically, what conduct may subject them to electronic surveillance.

b. Issuance Of A Preliminary Injunction Will Not Substantially Injure Defendants .

In contrast to the substantial irreparable harm facing Plaintiffs, there can be no credible claim of harm to Defendants. Defendants cannot be said to be "burdened" by a requirement to comply with the law.

c. The Balance Of Harm And The Public Interest Supports The Implementation Of A Preliminary Injunction.

The public interest prong is more than met because "there is an overriding public interest…in the general importance of an agency's faithful adherence to its statutory mandate."

Jacksonville Port Auth. V. Adams, 556 F.2d 52, 59 (D.C. Cir. 1977). The public has a substantial interest in Defendants following the law. *See, e.g., In re Medicare Reimbursement Litigation*, 414 F.3d 7, 12 (D.C. Cir. 2005 (Additional administrative burden "[would] not outweigh the public's substantial interest in the Secretary's following the law.")

Given Defendants' defects in complying with the law, and with basic notions of the right to privacy, in addition to their substantial contribution to significant constitutional violations, the public interest will be served if this court preliminarily enjoins Defendants from continuing their warrantless, unlawful participation in PRISM. In light of the fact that PRISM poses legitimate and unaddressed constitutional questions, a preliminary injunction to allow for the adjudication of these issues clearly serves the public interest. See *Tyndale House Publishers, Inc. v. Sebelius*, 904 F. Supp. 2d 106, 130 (D.D.C. 2012), (holding that "there is undoubtedly . . . a public interest in ensuring that the rights secured under the First Amendment . . . are protected"); *O'Donnell Const. Co. v. District of Columbia*, 963 F.2d 420, 429 (D.C. Cir. 1992) (holding that "issuance of a preliminary injunction would serve the public's interest in maintaining a system of laws" free of constitutional violations). See also *Seretse-Khama v. Ashcroft*, 215 F. Supp. 2d 37, 54 (D.D.C. 2002), (holding that the public interest is served by a court order that avoids "serious constitutional risks"); *N. Mariana Islands v. United States*, 686 F. Supp. 2d 7, 21 (D.D.C. 2009) (noting "the general public interest served by agencies' compliance with the law"); *Cortez III Serv. Corp. v. Nat'l Aeronautics & Space Admin.*, 950 F. Supp. 357, 363 (D.D.C. 1996) (public interest served by enforcing constitutional requirements).

C. PLAINTIFFS HAVE STANDING

Plaintiffs have standing under Article III. They have suffered an injury because they have been, at all material times, been consumers, users, and U.S. citizens who are subscribers, users, customers, and otherwise avail themselves to Facebook, Yahoo, Google, Microsoft, YouTube, AOL, PalTalk, Skype, Sprint, AT&T, and/or Apple. Plaintiffs' communications have already been monitored by the NSA under the Verizon Order and/or the PRISM program and their communications continue to be monitored. The injury is plainly traceable to the conduct they challenge—that is, to the NSA's collection of their call records as well as their internet communications and activities. And the injury would be redressed by the relief they seek—principally, an injunction against their mass warrantless surveillance tactics. The practice is akin to snatching every American's address book—with annotations detailing whom they spoke to, when they talked, for how long, and from where. The collection of Plaintiffs' communication records, specifically telephonic and online metadata belonging to Plaintiffs, is itself an injury sufficient for Article III; indeed, the collection of Plaintiffs' records constitutes a gross invasion of their privacy.

The Defendants have acknowledged that they have engaged in such metadata collection. Specifically, in regard to the PRISM surveillance program, the U.S. government has essentially confirmed the existence of the wide-ranging program known as PRISM, which allows the NSA to directly tap into consumer data from telephone and internet communication service providers, including Apple, Google, Yahoo!, Microsoft, Facebook, Skype, and others. *See, i.e.* HJC Hearing at 29:33–36:00 (testimony of John C. Inglis, NSA Deputy Director).

In addition, the Primary Order/Verizon Order indicates that every time the NSA queries the call-records database, it reviews everyone's records—Plaintiffs' among them—to determine

whether they, their contacts, or their contacts' contacts are connected to a phone number that the NSA deems suspicious. See Primary Order at 6–7, 11.

In any event, there can be no dispute that the bulk collection of Plaintiffs' call records gives them the stake in this litigation that Article III requires. Courts frequently analyze third-party challenges to records requests at the merits stage, rather than as a question of standing. See, e.g., *Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 270 (2d Cir. 1981).

Plaintiffs' First Amendment claim asserts a direct intrusion into their associational privacy, not just a chilling effect. Compl. ¶¶ 3, 35; This intrusion and the resulting injury is complete when the NSA collects Plaintiffs' communication records—regardless whether the surveillance ultimately dissuades any third party from communicating with them. Plaintiffs suffer a further, discrete injury because of the program's chilling effect on their key contacts and sources. The NSA's monitoring has and will continue to dissuade crucial contacts from associating with Plaintiffs.

The government seems to believe that there is something implausible about the notion that the NSA's surveillance might chill lawful expression and association, but "[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." *NAACP v. Alabama*, 357 U.S. 449, 462 (1958); *see also International Longshoremen's Asso. v. Waterfront Com. of New York Harbor,* 667 F.2d 267 (2d Cir. 1981); *Talley v. California*, 362 U.S. 60, 64 (1960).

Further, as the Supreme Court has observed, the definition of Fourth Amendment rights "is more properly placed within the purview of substantive Fourth Amendment law than within that of standing." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998); *accord Rakas v. Illinois*, 439 U.S.

128, 139 (1978). In any event, there can be no dispute that the bulk collection of Plaintiffs' call records gives them the stake in this litigation that Article III requires. Courts frequently analyze third-party challenges to records requests at the merits stage, rather than as a question of standing. *See, e.g.*, *Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 270 (2d Cir. 1981); *Koch v. Greenberg*, No. 07 Civ. 9600, 2009 WL 2143634, at *3 n.1 (S.D.N.Y. July 14, 2009).

1. Plaintiffs Have Demonstrated Irreparable Harm.

The Defendants conveniently ignore well-established case law holding that a colorable constitutional violation gives rise to a showing of irreparable harm. See *Mills v. District of Columbia*, 571 F.3d1304, 1312 (D.C. Cir. 2009) (a constitutional violation and loss of constitutional protections "'for even minimal periods of time, unquestionably constitutes irreparable injury'") (quoting *Elrod v.Burns*, 427 U.S. 347, 373 (1976)); see also *Seretse-Khama v. Ashcroft*, 215 F. Supp. 2d 37, 53 (D.D.C. 2002) (deprivation of constitutional protection "is an undeniably substantial and irreparable harm").

Plaintiffs have demonstrated the chilling effects of the Defendants' actions on the Plaintiffs. Plaintiff Charles Strange's son, Michael Strange, was a cryptologist technician for the National SecurityAgency ("NSA") and support personnel for Navy SEAL Team VI. Strange Aff. at ¶5. Plaintiffs have been vocal about their criticism of President Obama as commander-in-chief, his administration, and the U.S. military, particularly in regard to the circumstances surrounding the shoot down of the helicopter Michael Strange was in, which resulted in the death of Michael and other Navy SEAL Team VI and other special operations members. Strange Aff. at ¶¶9, 10. Plaintiffs hold press conferences and lobby in Washington, D.C. as advocates for their

son and to obtain justice for him, as well as to change the policies and orders of President Obama and the U.S. military's acts and practices, which contributed to their son's death. Strange Aff. at ¶10. Plaintiffs believe and advocate that the government is responsible, whether negligently or intentionally, for the death of their son. Strange Aff. at ¶9.

Defendants' mass data collection and call-tracking surveillance programs have directly and significantly impacted Plaintiffs, Charles Strange and his wife, Mary Ann Strange, and their abilities to communicate via telephone, email, or through any other means, given their valid concern that their confidential and private communications will be overheard or obtained by the NSA's surveillance program. Strange Aff. at ¶11. In fact, there have, on several occasions, been times when Plaintiff Charles Strange received text messages from friends, relatives, and others who later informed Plaintiffs that they had never sent him those messages. Strange Aff. at ¶14. Additionally, various other contacts have received text messages that seemingly appear to have been sent from Plaintiff Charles Stranges' phone number, even though he had never sent said messages. Strange Aff. at ¶15. More shocking, Plaintiff Charles Strange received an email that appeared to be from Michael. Strange Aff. at ¶13. After having the email reviewed and analyzed, it was determined that the email from his son was a hoax orchestrated by the NSA and the other Defendants. *Id*. In July of 2013, Mary Ann Strange was on the computer when it abruptly photographed her (through some form of abusive surveillance since her computer does not have a built-in camera), and falsely accused Plaintiff Mary Ann Strange of violating "Copyright and Related Rights Law." Strange Aff. at ¶17. Without a built-in camera, a computer user cannot take a picture of him or herself. Strange Aff. at ¶17. The intrusive and highly secretive surveillance that the government is performing on Plaintiffs has, justifiably, made them unable to communicate freely with friends, family, and other contacts, whether on the phone, through texts

messages, or via email and put them in great for themselves and their family. Strange Aff. at ¶18, 19. The government's surveillance activities have, consequently, chilled Plaintiffs' speech, and prohibited their ability to associate, to lobby Congress, and to be politically active. Strange Aff. at ¶¶18, 19, 20.

Plaintiff Klayman was similarly affected by the illegal actions of the Defendants. Plaintiff Klayman has gained national exposure and recognition through his strong public interest advocacy in furtherance of ethics in government and is publicly known as a civil and individual rights activists. Klayman Aff. at ¶4. As an attorney, Plaintiff Klayman routinely communicates by phone and by email with existing and potential clients about their legal representation, discusses confidential issues, and engages in legally privileged attorney-client and other privileged or private communications regarding ongoing legal proceedings. Klayman Aff. at ¶¶5, 10. Defendants' illegal surveillance directly and significantly impacts Plaintiff Klayman's ability to communicate via telephone, email, and otherwise, out of fear that his confidential, private, and often legally privileged communications will be overheard or obtained by the NSA's surveillance program. Klayman Aff. at ¶¶9, 10. Defendants' overly broad, highly intrusive illicit surveillance program, as well as their limitless indiscriminate invasion of Americans' privacy rights, undoubtedly will dissuade, and has dissuaded, potential clients and others from contacting Plaintiff Klayman, fearing reprisal, and, in addition, compromises Plaintiff Klayman's ability to serve their clients' interest and Freedom Watch's organizational goals. Klayman Aff. at ¶10.

Because he now fears that his telephone conversations and emails are being monitored -- because they are -- Plaintiff Klayman no longer engages in sensitive attorney-client conversations over the phone or by email. Exhibit 2 -- Supplemental Klayman Aff. at ¶13. Plaintiff Klayman has been forced to travel to meet with clients in order to ensure that his

conversations are indeed private. Supplemental Klayman Aff. at ¶14. This constant travel has come as a great expense to Plaintiff Klayman. *Id*.

Similarly, the Defendants have illegally violated the expectations of privacy of Plaintiffs Ferrari and Garrison who illegally and without a warrant had their internet records searched. Both Plaintiffs are prominent private investigators, who, as part of their work, communicate electronically, with associates and other members of the public regarding various matters, including work related discussions. Compl. ¶¶13, 14. Additionally, both Plaintiffs' emails contain private details, discussions and communications, and often include confidential documents and information. *Id*. Plaintiff Michael Ferrari is a subscriber, consumer, and user of Google/Gmail, Yahoo!, and Apple. Compl. ¶13. Plaintiff Matthew Garrison is a consumer and user of Facebook, Google, YouTube, and Microsoft. Compl. ¶14. Thus, both Plaintiffs have indisputably been subject to the NSA's warrantless searches of their online communications and internet activities. The Defendants' actions have similarly caused injury to these Plaintiffs as they can no longer communicate freely through email and telephone.

Plaintiffs have more than established the substantial harm that is being caused to them by the actions of the NSA through the PRISM program and the telephony metadata collection.

D. Standard of Evidence For a Preliminary Injunction.

Preliminary Injunctions are customarily granted on the basis of procedures that are less formal and evidence that is less complete than in a trial on the merits, and therefore the party moving for the preliminary injunction is not required to prove his case in full at a hearing. *See Attorney General of Oklahoma v. Tyson Foods, Inc*., 565 F3d769 (10th Cir. 2009). The Plaintiffs have not had the opportunity to conduct discovery and once the lawsuit moves to the

discovery phase the Plaintiffs will be able to determine to what extent Defendants have in fact been conducting illegal surveillance of Plaintiffs.

Plaintiffs have presented the statements of key whistleblower Edward Snowden. Pursuant to Federal Rules of Evidence Rule 804, the Statements of Edward Snowden are not excluded by the hearsay rule if the declarant is unavailable as a witness: "Declaration Against Interest: A statement which was at the time of its making so far contrary to the declarant's pecuniary or proprietary interest, or so far tended to subject the declarant to civil or criminal liability, or to render invalid a claim by the declarant against another, that a reasonable person in the declarant's position would not have made the statement unless believing it to be true. A statement tending to expose the declarant to criminal liability and offered to exculpate the accused is not admissible unless corroborating circumstances clearly indicate the trustworthiness of the statement."

Plaintiffs have additionally requested the authentication of several formerly classified documents in the form of a *Touhy* request that has been submitted to the NSA. *See Touhy v*. *Ragen*, 340 U.S. 462 (1951); Exhibit 3 -- NSA *Touhy* request.

E. Plaintiffs' Claims Are Not Precluded By Statute.

Plaintiffs are capable of enforcing the violations of 18 USC § 2702 through the Administrative Procedures Act ("APA"), 5 USC § 706. Defendants argue that the provision allowing recipients to challenge Section 215 orders, added in 2006, manifests a congressional intent to bar all other claims and relief under this section. 50 U.S.C. § 1861(f). Yet this argument simply turns Congress's attempt to clarify the availability of one remedy into an attempt to subtract the rest of the remedies. Defendants can cite to no evidence of such an intent. As the Supreme Court observed last year, "if the express provision of judicial review in one section of a

long and complicated statute were alone enough to overcome the APA's presumption of reviewability for all final agency action, it would not be much of a presumption at all." *Sackett v. EPA*, 132 S. Ct. 1367, 1373 (2012). The government argues that the addition of 50 U.S.C. § 1861(f) in 2006 was a deliberate effort to imit the right to contest the legality of Section 215 production orders to recipients, but the legislative history shows that Congress added 50 U.S.C. § 1861(f) merely to "clarify" an already-existing remedy. In doing so, Congress gave no indication that it intended to displace other existing remedies, including those provided by the APA. See H.R. Rep. 109-174, pt. 1, at 6, 77, 106 (repeatedly describing the addition of this subsection as an effort to "clarify" the statute). Indeed, at the time, the government concurred in the view that this addition did not represent a significant change in the law. *See, e.g.*, Implementation of the USA PATRIOT Act: Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Security, Comm. on the Judiciary, 109th Cong. at 106 (2005) ("Patriot Act HJC Hearing") (testimony of Kenneth Wainstein, U.S. Attorney for the District of Columbia).

This change was made for a simple reason: Congress made explicit recipients' ability to go before a judge to challenge a production order, as is customary with ordinary subpoenas. See, e.g., Fed. R. Crim. P. 17(c); Patriot Act HJC Hearing at 65 (statement of Robert Khuzami) (amendment designed to "place Section 215 proceedings on a par with grand jury proceedings"). This was done because the legal process available to recipients of records demands under a similar statute, 18 U.S.C. § 2709 (national security letters), had been the subject of litigation. See, e.g., *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 507 (S.D.N.Y. 2004); Patriot Act HJC Hearing at 105-06, 140-42 (discussing Doe). But in the course of clarifying the procedures for raising such an objection under Section 215, Congress nowhere altered—or even considered—the APA's background presumption, especially as it applies to the subjects of record requests. As a matter

of statutory structure, nothing in the recipient-review procedure bars the traditional APA review that Plaintiffs seek here—rather, they are complimentary remedies. Recipients may challenge a Section 215 production order but, as with subpoenas, this does not inevitably imply an intent to bar the subject of a records request from bringing her own challenge.

Courts routinely allow third parties to contest subpoenas on grounds other than privilege—including their asserted privacy interests. *Arias-Zeballos v. Tan*, No. 06 Civ. 1268, 2007 WL 210112, *1 (S.D.N.Y. Jan. 25, 2007) (listing cases). Relying on *Block v. Community Nutrition Institute*, 467 U.S. 340, 349 (U.S. 1984), the Defendants argue that because Section 215 provides for recipient challenges, it impliedly precludes judicial review "at the behest of other persons," like Plaintiffs.

But as courts have recognized, this assumption is too simplistic. In particular, the D.C. Circuit has cautioned against reading *Block* "too broadly," especially where the interests of the various parties may diverge or the statute bears directly on the class to which the plaintiff belongs. *Ark. Dairy Co-op Ass'n, Inc. v. U.S. Dep't of Agr.*, 573 F.3d 815, 822–23 (D.C. Cir. 2009). The court did so in a case involving the very same statute that the Supreme Court interpreted in *Block*, finding that the APA afforded a right of review to milk producers despite the fact that the statutory scheme at issue granted such a right only to milk handlers. *Id.* at 823; *see Koretoff v. Vilsack*, 614 F.3d 532, 536–40 (D.C. Cir. 2010); *Council for Urological Interests v. Sebelius*, 668 F.3d 704, 710 (D.C. Cir. 2011) (distinguishing *Block* where agency action had "direct" and "substantial" impact on plaintiffs); see also *Pottawatomi*, 132 S. Ct. at 2209 (rejecting comparison to *Block*). Even in *Block* itself, the Supreme Court evaluated the availability of judicial review under the APA by taking into account a proxy's willingness to pursue a plaintiff's interests. 467 U.S. at 352.

These concerns apply to Section 215. Indeed, "no recipient of any Section 215 Order has challenged the legality of such an Order." See 2013 FISC Opinion at 15– 16. That is perhaps because recipients are shielded from liability for complying with such orders, see 50 U.S.C. § 1861(e), and thus their interests diverge from those of the orders' subjects. See Strengthening Privacy Rights and National Security: Hearing Before the S. Comm. on the Judiciary, 113th Cong. at 4 (2013), http://bit.ly/19CVPgl (statement of Marc Zwillinger, Yahoo! counsel) (describing "institutional pressures and procedural disincentives against levying a [provider] challenge" to a FISC order).

The cases discussed above demonstrate that a statute's silence with respect to one class of plaintiffs or claims does not invariably imply that those plaintiffs have no road to court. The government's "effort to transform silence into implicit prohibition would seriously undermine Congress's effort in the APA to authorize specific relief against the United States." *U.S. Army Corps of Eng'rs*, 667 F.3d at 775. It takes more to show "clear and convincing evidence" of Congress's intent to strip the APA's remedies and preclude review. For instance, in *Dew v. United States*, 192 F.3d 366, 371–74 (2d Cir. 1999), the Second Circuit carefully analyzed the comprehensiveness of the statutory scheme at issue, the express signs of intent in the legislative history, and the parallel structure of a similar statute—ultimately concluding that each of these factors favored preclusion. In this case, one can hardly say the same.

There are clear examples of when Congress has explicitly intended to create a comprehensive and exclusive remedial scheme, such as in the Stored Communications Act, 18 USC §§ 2701–2712. In *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114 (E.D. Va. 2011), the court considered the carefully drawn remedies that the SCA makes available to internet-service subscribers and it found that the statute barred a

Twitter subscriber's pre-execution challenge to certain disclosure orders, pointing to the SCA's plain statement that "[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for non-constitutional violations of this chapter." *Id*. at 129 (quoting 18 U.S.C. § 2708). Contrary to this holding, Congress never intended to preclude claims under Section 215, and nothing in the language of the statute or the legislative history proves otherwise.

III. CONCLUSION

As set forth in the accompanying proposed memorandum opinion and order, the Plaintiffs ask for the following: (1) that the Court preliminary restrains and enjoins Defendant NSA, its agents, servants, employees, attorneys, and all others in active concert or participation with the NSA, from implementing surveillance procedures, tactics, and programs that exceed statutory authority and constitutional provisions; (2) that the NSA is respectfully ordered to comply with any and all laws regarding the government's authority, power, and limits in conducting such mass warrantless domestic surveillance, including, but not limited to, Section 215 of the Patriot Act, Section 702 of the FISA Amendment Act, and the provisions of the U.S. Constitution; and (3) that within twenty (20) days of this date, the NSA submit declarations and any pertinent records, reports, and/or other documents to the Court regarding compliance with any and all minimization procedures implemented to prevent further warrantless collection of records belonging to U.S. citizens without reasonable suspicion or probably cause, any and all incidences of non-compliance, identification of any and all "targets" subject to the NSA's surveillance, and all other relevant reports, risk assessments, memoranda, and other documents. In the event that the records, reports, and/or other documents contain classified information, Defendants shall present such information in camera to the Court.

Dated: November 14, 2013

Respectfully submitted,

/s/ Larry Klayman

Larry Klayman, Esq.
Attorney at Law
D.C. Bar No. 334581
2020 Pennsylvania Ave. NW, Suite 800
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 14th day of November, 2013, a true and correct copy of the foregoing Reply in Support of Motion for Preliminary Injunction (Civil Action Nos. 13-cv- 851 & 13-cv-881) was submitted electronically to the District Court for the District of Columbia and served via CM/ECF upon the following:

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
(202) 514-3358
Email: James.Gilligan@usdoj.gov

James R. Whitman
U.S. DEPARTMENT OF JUSTICE
P.O. Box 7146
Washington, DC 20044
(202) 616-4169
Fax: 202-616-4314
Email: james.whitman@usdoj.gov

Randolph D. Moss
WILMER CUTLER PICKERING HALE & DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6640
Fax: (202) 663-6363
Email: randolph.moss@wilmerhale.com

Attorneys for Defendants.

Respectfully submitted,

/s/ *Larry Klayman*
Larry Klayman, Esq.
D.C. Bar No. 334581
Klayman Law Firm
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006
Tel: (310) 595-0800