IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, *et. al* Plaintiffs, v. BARACK HUSSEIN OBAMA II, *et. al* Defendants.	Civil Action Nos. 13-cv-851 and 13-cv-881

PLAINTIFFS' SUPPLEMENTAL BRIEF ON JURISDICTION AND STANDING

At oral argument on November 18, 2013, the Court *sua sponte* granted leave for the parties to file supplemental briefs on the issues of jurisdiction and standing. Plaintiffs appreciate the Court's diligence in deciding these cases on preliminary injunction motions.

I. Introduction

The National Security Agency (NSA) has carried out against the U.S. citizenry the most egregious violations of constitutional rights in American history. As the Court itself recognized during the status conference of October 31, 2013: "This is a case at the pinnacle of public national interest, pinnacle." Transcript of October 31, 2013 at pp. 7.

Indeed, never before in the history of the United States has a government agency, in this case the NSA, literally broken into and accessed the private phone, internet and social media records of nearly the entire American population, which exceeds 300 million persons. By way of contrast, President Richard Nixon broke into just the Watergate office complex, for which he was forced to ultimately resign. The NSA's massive break-in of over 300

million Americans' private communications did so without regard to the statutory and constitutional limitations (set forth in 50 U.S.C. § 1861 and 50 U.S.C. § 1881) which "govern" government access to records which have some nexus to crime and terrorist activities and are relevant as part of an authorized investigation limited in time – not continuing well into the future as is the case with the NSA's illegal actions. Indeed, Congress adopted the Foreign Intelligence Surveillance Act (FISA) after years of in-depth congressional investigation revealing that the executive branch engaged in widespread illegal, warrantless surveillance of U.S. citizens "who engage in no criminal activity and who posed no genuine threat to the national security." S. Rep. No. 95-604, pt. 1, at 8 (1977), reprinted in 1978 U.S.C.C.A.N. 3904, 3909 (quotation marks omitted).

As counsel for the Plaintiffs argued at oral argument on their motions for preliminary injunction, only this Court stands in the way of continued tyranny by the NSA over the American people. Counsel stated:

> "Briefly, [Number one] your Honor, with regard to what is at issue, the Government has been forced to admit despite a pattern of lying that it is collecting the metadata of 300 million plus Americans. That's a fact. It is not in dispute.
>
> Number two, Judge Bates – and we have cited his order in our briefs – has ruled that the monitoring system [to prevent abuse by the NSA] doesn't work. [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.]
>
> Number three, we have a situation here where if we are to accept what they [NSA] says as true and the Government now has a history of lying, as your Honor pointed out at the status conference, we have got to go to discovery so lets go to discovery and find out what is going on here.
>
> Number four, my clients [and me] have in affidavits, in original affidavits, supplemental affidavits set forth a real injury here. They have had their text messages, myself included messed with [us]. They have had their computers

tampered with susceptible to removing information. They are in the line of fire. I am in the line of fire. Not only am I head of a public interest group, but I am a fierce advocate against this administration. I have sued the NSA. Mr. Strange his son was an NSA cryptologist and extremely critical of the NSA and extremely critical of the NSA and the military for what happened to his son and has gone very public. I have a lawsuit for him in that regard. Attorney-client privilege, work product and other privileges are at stake.

With regard to *Smith* [*Smith v. Maryland*, 442 U.S. 735 (1979)], your Honor has it right. Not only is it outmoded, but it severely [is] limited to one little narrow part of date and the order was finite in time, it was [for] only two days, and it was also limited to a criminal investigation at this time. Who knows in the future with the way things are going.

But the reality is that the IG himself, the NSA's own IG, in that report and [the] documents [that] are in the record, the report finds [over] 2,700 violations of these statutes since 2012 is there, plus 12 violations that we know of people getting into the private affairs of their boyfriends and girlfriends and husbands and wives. Just think what the potential is for anything else.

Your Honor, with regard – and this was overlooked. No one wants to talk about Mr. Snowden here for obvious reasons, but I have a bench brief. I would like to provide it to your honor.

Mr. Snowden made admissions against interest. By making these admissions these statements against interest, he subjected himself to criminal prosecution. He is now a fugitive from justice, has to live in Russia for fear that he might be killed in this country. [Implicating Rules 804(b)(3) and 801 of the Federal Rules of Evidence.]

And these allegations set forth – they are not allegations, they are admissions – that the NSA did have access and does have access on an ongoing basis to the metadata of 300 million Americans such that if the NSA wants to coerce and intimidate you, even you, a Federal judge, they can get into it. [*Id*.]

Consequently, Snowden's statements come into evidence. The binder [*see* Exhibit 1 to this brief] has documents where admissions by the Government, they are public documents now, they don't even have the integrity to come forward and authenticate these documents. Heads I win. Tails you lose. We are the Government. You people are nothing. You don't matter to us at all. We will do what we want and have all the cards and heck with you, you take a hike.

And there is not one American that can pick up his phone or send an e-mail message or go on Facebook, YouTube or Skype and now not think he is being surveyed, but here we have standing because we set forth concrete

> information in affidavits of exactly what is going on. If the Government wants to refute it, let them take our depositions. We will be very happy to take theirs.
>
> So, your Honor, we are appreciative of your time but we look to you to protect not just Plaintiffs but the American people against the NSA which has frankly been out of control and is creating a situation where the American people feel that their Government is against them and can destroy them and will keep them submissive such that they can't even complain about their grievances and, in that respect, we are in worse shape than we were in 1775.
>
> Let me add one point in that regard. As we said in our briefs, if the NSA had been in existence and available to King George, the Founding Fathers would have never made it Philadelphia for the Declaration of Independence. They would have been picked up, arrested and executed. Thank you. Hearing of Transcript of November 18, 2013 (Tr.) at pp. 46-60.

II. The Law

A. THIS COURT HAS JURISDICTION.

While the NSA Defendant, at oral argument, conceded that this Court has jurisdiction to hear this case and thus has the authority to issue a preliminary injunction, jurisdiction is also supported through both statutory and case law. So too does the brief of the Solicitor General that was submitted in a collateral case that had been filed by the Electronic Privacy Information Center before the U.S. Supreme Court. As usual, the NSA Defendant, having been caught lying on numerous occasions to the Foreign Intelligence Surveillance Court (FISC) and Congress, speaks out of both sides of its mouth – consistent with the pattern of continuing its illegal unconstitutional conduct at issue.

The lawyer for the NSA, James Gilligan, admitted that: "The Supreme Court has held many times in such cases as *Block v. Community Nutrition Institute* [467 U.S. 340 (1984)] that a statute can implicitly preclude other types of review; but when it comes to precluding review of constitutional claims, the Court explained in *Webster v. Doe* [486 U.S. 592 (1988)]

that it insists on a clearer expression on the part of Congress to preclude review." Transcript of November 18, 2013 at 27.

Clearly and unequivocally, there is nothing in the Foreign Intelligence Surveillance Act (FISA) that precludes review by this Court of an illegal and unconstitutional search of Plaintiffs' telephonic, online, and social media metadata.

Consistent with the NSA Defendant's admission, it is black-letter law that federal district courts have authority to review and rule upon the legality and scope of FISC orders. While this is a case of first impression for this Court – arising from the leaked evidence of Edward Snowden and the forced admissions of James Clapper, Director of National Intelligence and reports of Inspector General, the nation has just learned of the rampant illegality at issue – district courts routinely review NSA warrantless and other surveillance activities in the context of motions to suppress evidence. As set forth in 18 U.S.C. § 1806(c), (d), (e) and (f), district courts clearly provide private litigants an avenue of redress:

> (c) Notification by United States
> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.
>
> (d) Notification by States or political subdivisions
> Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or

> other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.
>
> (e) Motion to suppress
> Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—
> (1) the information was unlawfully acquired; or
> (2) the surveillance was not made in conformity with an order of authorization or approval.
> Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.
>
> (f) In camera and ex parte review by district court
> Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

Case law is consistent with this statutory scheme. For instance, in *United States v. Rosen*, 447 F. Supp. 2d 538 (E.D. Va. 2006), defendants, officials of a pro-lobbying organization, were charged with espionage for conspiring to transmit information relating to

national defense to those not authorized to receive it. In the course of its investigation, the government sought and obtained orders issued by FISC pursuant to 50 U.S.C. § 1801 *et seq*. of FISA, authorizing certain physical and electronic surveillance. Defendants moved to suppress this evidence and the Eastern District ruled upon these motions, just as this Court has the authority and power to rule on Plaintiffs motions for preliminary injunction in these cases. *See also In re: Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008).

In addition, district courts have absolute authority to hear claims that a statute or its implementation is unconstitutional. The U.S. Constitution directly vests the district court with original jurisdiction to hear these cases. 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, § 2.

Jurisdiction is also proper under 28 U.S.C. § 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 U.S.C. § 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 U.S.C. § 1331; *see also 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 FISA 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 U.S.C. § 1331.

Finally, as the Solicitor General of the United States admitted on behalf of Defendant NSA in a brief filed before the U.S. Supreme Court in a related case concerning Verizon, styled *In re Electronic Privacy Information Center*, Petitioner, Case No. 13-58:

> "Nor does the fact that the FISC has approved the Telephony Records Program suggest that review must begin in this Court and not in a district court. In general, no constitutional or procedural bar prohibits a plaintiff from seeking injunction relief that, if granted, would conflict with an order previously entered in another proceeding to which plaintiff was not a party. *See Taylor v. Sturgell*, 553 U.S. 880, 892-893k (2008); *Martin v. Wilks*, 490 U.S. 755, 761 (1989)."

On this basis, the U.S. Supreme Court presumably denied the petitioner's writ, deferring to this Court and the ACLU court in the Southern District of New York, at the urging of the Obama Justice Department. See Exhibit 2 – Brief of the Solicitor General at pp. 20-23.

In sum, this Court has absolute jurisdiction to hear these companion cases and issue preliminary injunctions ordering the NSA to obey the law and not engage in illegal and unconstitutional searches of U.S. citizens, such as Plaintiffs, who are not subject to an authorized investigation for any criminal conduct or any communications overseas with foreign interests with connections to terrorists or terrorism.

B. PLAINTIFFS HAVE STANDING.

Plaintiffs have standing pursuant to Supreme Court case law and Article III of the U.S. Constitution. Ironically, and as yet another example of the NSA's dishonest approach, Defendant NSA argue that the seminal Supreme Court case of *Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147-50 (2013) supports its position that no standing is present. But, to the contrary, *Clapper* stands for the proposition that Plaintiffs indeed have standing. It is not a distinguishable case; rather, while denying standing to the appellants, the

Supreme Court in *Clapper* clearly sets forth the criteria for plaintiffs to have standing in national security surveillance cases under section 702 of the FISA of 1978 and 50 U.S.C. §1881a, added by the FISA Amendments Act of 2008. This standard for standing also logically applies to section 215 of FISA, which is also at issue here.

In *Clapper*, a divided Supreme Court held that Plaintiffs lacked standing to bring their constitutional challenge to the FISA Amendments Act of 2008. However, the ultimate finding for the Defendants in *Clapper* is wholly inapplicable here. There, the Court reached that conclusion not because the plaintiffs failed to demonstrate that their communications had been retrieved from government databases, but because the plaintiffs failed to demonstrate that their communications had been collected at all. *Clapper* at 1147-50. In fact, in *Clapper*, the NSA Defendants did not dispute that the plaintiffs would have standing if they could show that the NSA Defendants had collected their communications. Here, there is no doubt that Defendant NSA has collected, reviewed, and accessed Plaintiffs metadata. It has been forced to admit that it has done so.

Indeed, in *Clapper*, the Supreme Court found that to have standing plaintiffs must merely show that "the injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Monsanto Co. v. Geertson Seed Farms*, 130 S. Ct. 2743, 2752, 177 L. Ed. 2d 461, 471 (2010). "(T)hreatened injury must be 'certainly impending' to constitute injury in fact,' and 'allegations of possible future injury' are not sufficient." *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990). Clapper at 1140-41.

In the instant cases, the injuries to Plaintiffs, as set forth below, are not speculative and are traceable to the NSA Defendant. And they are both "certainly impending" and

"redressable" through preliminary and permanent injunctions. Here, based on the admissions of Edward Snowden and his NSA, it is uncontroverted that the agency has obtained the metadata cell phone, internet and social media records of not just Plaintiffs, but also nearly 300 million Americans having no connection to foreign intelligence, as is required by the act, and who are not under an authorized investigation for crimes or ties to terrorism. Thus, the injury is concrete, particularized and imminent; that is "certainly impending." And, the injury is traceable to the Defendant NSA.

In this regard, not only have Plaintiffs shown in their **unrefuted** affidavits that they have been spied upon by the Defendant NSA through the indiscriminate collection of and access to metadata, but the expert testimony of Edward Felten, also **unrefuted**, shows that the collection of this metadata allows the agency to violate the private lives and professions of the Plaintiffs as if it was actually listening or reading the content of their communications. The metadata is indisputably in the possession of the agency. This was not necessary if the NSA had no intention of using it, as the metadata could have been left with the third party cell phone and Internet providers until there was a showing of government need for it.

Moreover, both the relevant statutes 215 and 702 apply to the use of surveillance to intercept foreign intelligence sources. As expert Felten testifies and as we know from the NSA admissions through Snowden and otherwise, its illegal surveillance collected and accessed metadata on purely domestic plaintiffs and putative plaintiffs without any connection to foreign intelligence gathering related to terrorism. This is a clear violation of FISA.[1]

[1] It is a well established principle that "[t]he actual or threatened injury required by Article III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing . . ." *Warth v. Seldin*, 422 U.S. 490, 500, 95 S. Ct. 2197, 2206, 45 L.Ed.2d 343 (1975) (citations

Finally, the documented history of the NSA's lying to Congress and the courts and its huge systematic violations of FISA, as evidenced in the report of its own Inspector General, which found over 2700 violations since 2012 and 12 violations of the agency's personnel spying on their so-called lovers, raises an evidentiary inference that they have violated the act with and injured Plaintiffs. Letter from National Security Agency Inspector General George Ellard to Sen. Charles E. Grassley (Sept. 11, 2013); 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. It is well established that a pattern of illegal conduct gives rise to such a strong evidentiary inference that it has occurred with regard to Plaintiffs. *See Alexander v. FBI*, 186 F.R.D. 154, 158 (D.D.C. 1999) ("This [**7] line of discovery is appropriate because plaintiffs may seek to create the inference that if the White House misused government information for political purposes in the case of the Tripp release, such evidence may be circumstantial evidence of the similar conduct alleged in plaintiffs' complaint.").

Moreover, even under a standard analysis that does not apply specifically to FISA, as in *Clapper*, Plaintiffs still have demonstrated standing under this general analysis applicable to constitutional law violations in general. For instance, Article III states, "The judicial power shall extend to all Cases . . . [and] Controversies . . .", and thus provides federal courts jurisdiction if the case brought before it meets the case-or-controversy requirement. U.S. Const. Art. III, § 2. The constitutional requisites for Article III are that Plaintiffs must

---

omitted). The Supreme Court has reiterated time and time again the principle that Congress may legislatively create rights, and the invasion of these statutory rights, constitutes the requisite injury for Article III standing purposes. *See also O'Shea v. Littleton*, 414 U.S. 488, 495 (1974) ("We have previously noted that Congress may enact statutes creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute.") *Linda R.S. v. Richard D.*, 410 U.S. 614, 617 (1973).

personally have suffered some actual or threatened injury that can fairly be traced to the challenged action of Defendants and that the injury is likely to be redressed by a favorable decision. *Valley Forge Christian College v. Americans United*, 454 U.S. 464, 472 (1982); *Allen v. Wright*, 468 U.S. 737, 751 (1984); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Plaintiffs have suffered injury because they are current Verizon subscribers[2] whose communications have already been monitored by the NSA and will continue to be monitored until injunctive relief is granted. The injury is plainly traceable to the Defendants conduct – that is, to the NSA's collection of their call records. Finally, the relief they seek which is a preliminary injunction against the mass collection of their records would redress plaintiffs' injuries.

It has been long established that the loss of constitutional freedoms unquestionably constitutes irreparable harm. *Elrod v. Burns*, 427 U.S. 347, 373 (1976). In *Elrod*, the Supreme Court held that a constitutional violation and loss of constitutional protections "for even minimal periods of time, unquestionably constitutes irreparable injury." *Id*; *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009); *see also Seretse-Khama v. Ashcroft*, 215 F. Supp. 2d 37, 53 (D.D.C. 2002).

The legal threshold for proving violations of the First Amendment with regard to freedom of association is low. 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. Thus, the courts have subjected such investigative methods

[2] Defendant NSA has presented no evidence, nor has Defendant Verizon, that Plaintiffs have not sued the correct Verizon entity. The allegations of the relevant Complaints must be taken as true. As is true in the ACLU's case which also seeks preliminary injunctive relief, Verizon is not at issue at this stage of the proceeding in any event, as the Court has limited its review at this stage to the government Defendant NSA and its named officials.

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 government 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*, 427 U.S. at 362 (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 government interference.").

The Supreme Court has repeatedly emphasized the importance of preserving constitutional rights of advocacy groups, recognizing that the government's surveillance and investigatory activities infringe on associational rights protected by the First Amendment. In *Gibson*, the court ruled, "[t]he First and Fourteenth Amendment rights of speech and free association are fundamental and highly prized and 'need breathing space to survive.'" *Gibson v. Florida Legislative Investigation Committee*, 372 U.S. 539, 544 (1963), citing *NAACP v. Button*, 371 U.S. 415, 433 (1963). Similarly, 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 less intrusive surveillance than is present here. The 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." *Id*. at 462.

Here, the NSA's broad sweeping surveillance program raises to a much greater extent the same associational harm as in *NAACP*, since Plaintiffs are particularly vulnerable to this type of surveillance and the information collected and accessed, given their professions, political activism, public personas, and activities which often involve highly confidential matters and privileged information. In short, the NSA's collection and access and use of metadata in the instant cases is even more highly violative of associational privacy rights than in *NAACP*, as testified to by expert Edward Felton.

The injury-in-fact requirement for standing simply states, "that the party seeking review be himself among the injured." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 563 (1992). Defendant NSA has injured Plaintiff Klayman in ways which include but are not limited to: (1) directly and significantly impacted Plaintiff Klayman's abilities to communicate via telephone, email, and otherwise, given the concern that confidential, private, and legally privileged communications are obtained and accessed, are particularized, actual or imminent and fairly traceable to the NSA's surveillance program, and are thus applicable to Plaintiff, Plaintiff's contacts and clients, whistleblowers, and others concerning government abuses and corruption; Klayman Affidavit ¶ 10 (hereinafter Klayman Aff.) (2) various contacts of Plaintiff Klayman have received text messages generated by NSA Defendant that purport to have been sent from Plaintiff Klayman's cell phone number, even though Plaintiff Klayman never sent the messages. *Id*. at ¶ 11 (3) the coercive tactics by the NSA have compromised Plaintiff Klayman's security and relationships with clients,

whistleblowers, and other sources of government abuses and corruption, and silenced Plaintiff and his legal advocacy; *Id*. at ¶ 12 (4) effectively chilled Plaintiff Klayman's freedom of speech and association, protected by the First Amendment to the U.S. Constitution, as he is unable to speak on the telephone with clients, friends, and other relationships because his attorney/client communications, work product, and other legal privileges and rights are breached, compromised and disclosed to a government which Plaintiff Klayman is adverse to and which has the potential to act maliciously towards Plaintiff; *Id*. at ¶ 13 (5) forced Plaintiff Klayman to travel to potential clients' and current clients' locations knowing that the NSA and other government agencies with which it collaborates are surveying Plaintiff Klayman; *Id*. at ¶ 14 (6) chilled potential clients from contacting Plaintiff Klayman because they are aware of the NSA's illegal surveillance program; *Id*.

Plaintiff Strange, father of a murdered cryptologist technician for the NSA and support personnel for Navy SEAL Team VI, and Plaintiff Strange's wife, Plaintiff Mary Ann Strange, have been injured by the Defendant NSA's illegal actions in ways which include but are not limited to: (1) directly and significantly impacted their ability to communicate via telephone, email, and other mediums because of their criticism of Barack Obama as Commander-in-Chief, his administration, and the U.S. military regarding the circumstances surrounding the shoot-down of their son's helicopter by the Taliban; Strange Affidavit ¶ 9, 11 (hereinafter Strange Aff.) (2) Plaintiff Strange received an email purportedly from his deceased son, Michael, which he believes, based on the totality and continuing pattern of the circumstances, that the NSA Defendant was responsible for; *Id*. at ¶ 13 (3) Plaintiff Strange has received text messages from friends and relatives who have told him after they did not

send to him; *Id*. at ¶ 14 (4) since the death of Plaintiff Strange's son and his criticism of the current administration, Plaintiff Strange has received text messages from indiscriminate numbers, all with one, two, three, four, and five digits. Plaintiff Strange contacted Verizon various times and its employees stated that there is no record of the text messages being sent or received; *Id*. at ¶ 16. (5) in July of 2013, Plaintiff Mary Ann Strange was using her computer in the privacy of her own home when it abruptly photographed her face (through some form of abusive surveillance as Plaintiff Mary Ann Strange's computer does not have a built-in camera), and falsely accused Plaintiff Mary Ann Strange of violating "Copyright and Related Rights Law." Without a built-in camera, the computer user cannot take a picture of him or herself; *Id*. at ¶ 17. (6) Plaintiff Strange is afraid to communicate with his friends, family and other contacts. Plaintiff Strange is in fear of his safety, his family's safety, immediate bodily harm, and even death because of his staunch commitment to find justice for his deceased son and his criticism of the government; *Id*. at ¶ 18. (7) Plaintiff Strange is no longer able to exercise his constitutionally protected right to speak freely on the phone, through text messages and email; *Id*. at ¶ 19 (8) Plaintiff Strange is no longer able to associate, as protected by the First Amendment of the U.S. Constitution, to lobby Congress, to be politically active, and to communicate freely and openly with his counsel, Plaintiff Klayman.

As compelling, David M. Siler, a computer expert holding over one hundred and thirty certifications granted by various software and hardware manufacturers, specializing in configuring and deploying global anti-virus and anti-spyware solutions, in an attempt to restore Plaintiff Strange's workstation, determined that the viruses, spyware and keystroke loggers were implanted on the computer after Plaintiff Strange inserted a disc that was given

to him by the U.S. military regarding his son's death. Siler Affidavit ¶ 4, 5, 12 (hereinafter Siler Aff.) Siler found that the viruses had been installed on the workstation on the same date and time that Plaintiff Strange had inserted the disc into his computer to view the crash report of his son. *Id*. at ¶ 12. Because of the enormity of the viruses, Siler was forced to use five different tools to remove the viruses, malware and spyware which took over four hours to complete. *Id*. at ¶ 13. After he removed the various viruses, he then scanned the disc drive of the workstation and discovered that the viruses originated from the disc drive and not the workstation.

Edward W. Felten, a Professor of Computer Science and Public Affairs, as well as Director of the Center for Information Technology Policy, at Princeton University, filed sworn declarations providing evidence and expert testimony of the sensitive and intrusive nature of metadata, particularly when obtained in the aggregate, as occurred here. Declaration of Felton ¶ 1 (hereinafter Decl. of Felten). Following the disclosure of the Verizon Order, Edward Snowden and other NSA officials admitted that the NSA's acquisition of phone records are not limited to Verizon but that the NSA is maintaining a record of the metadata associated with nearly every telephone call originating or terminating in the United States. *Id*. at ¶ 10. Felton's declaration proves that metadata is easy to analyze, telephony metadata reveals content, and aggregated telephony metadata is even more revealing and invasive in relation to content than simply listening in on calls – the traditional method of wiretapping.

The structured nature of metadata makes it very easy to analyze massive datasets using sophisticated data-mining and link-analysis programs. That analysis is greatly facilitated by technological advances in computing, electronic data storage, and digital data

mining. These advances have radically increased the ability to collect, store, and analyze personal communications, including metadata. *Id*. at ¶ 22. The newfound data storage capacity has led to new ways of exploiting the digital record. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits, and behaviors. As a result, individual pieces of data that previously carried less potential to expose private information may now, in the aggregate, reveal sensitive details about people's everyday lives – details that people had no intent or expectation of sharing. *Id*. at ¶ 24.

As Felton's declaration proves, telephony metadata is extremely revealing and invasive, both at the individual level and, especially, in the aggregate. *Id*. at ¶ 38. Although the NSA Defendant falsely wants people to believe that metadata might be little more than information regarding dialed numbers, analysis of telephony metadata in fact reveals information that could traditionally be obtained by examining the contents of communications. Metadata is often a proxy for content. *Id.* at ¶ 39. Certain telephone numbers are used for a single purpose, such that any contact reveals basic and often sensitive information about the caller. Examples include support hotlines for victims of domestic violence, rape, suicide, gay and lesbian teenagers, and those who suffer from various forms of addiction. *Id*. at ¶ 40.

In fact, telephony metadata reveals information that is even more sensitive than the contents of the communication. Recently, wireless telephone carriers have partnered with non-profit organizations in order to permit wireless subscribers to donate to charities by sending a text message from their telephones. These systems require the subscriber to send a specific text message to a special number, which will then cause the carrier to add that

donation to the subscriber's monthly telephone bill. *Id*. at ¶ 43. In all these cases, the most significant information – the recipient of the donation – is captured in the metadata, while the content of the message itself is less important. The metadata alone reveals the fact that the sender was donating money to his or her church, to an abortion clinic, or to a particular political campaign. *Id*. at ¶ 45.

When call metadata is aggregated for information across time, it is an even richer repository of personal and associational details. *Id*. at ¶ 47. Analysis of metadata can reveal the network of individuals with whom people communicate. By building a social graph of this sort which maps all of an organization's telephone calls over time, one could obtain a set of contacts that includes a substantial portion of the group's membership, donors, political supporters, and confidential sources. *Id.* at ¶ 48.

With an organization like Freedom Watch and its founder and general counsel, Larry Klayman, aggregated metadata reveals sensitive information about the internal workings of the organization and Plaintiff Klayman and about their external associations and affiliations. Plaintiff Klayman's metadata trail reflects his relationships with his clients, his legislative contacts, his donors, and the prospective whistleblowers that call him and his organization. And, two of Plaintiff Klayman's and Freedom Watch's clients are, not coincidentally, Plaintiffs Charles and Mary Ann Strange.

III. Conclusion

These cases before this Court seek to redress the most egregious and outrageous wholesale violation of the privacy and constitutional rights of not just Plaintiffs, but nearly 300 million other Americans who have done nothing wrong, committed no crime and are not

in contact with foreign intelligence sources and terrorists – and thus not under an authorized investigation as required by FISA.

This Court is being asked by the Plaintiffs to simply enter preliminary injunctions to hold Defendant NSA to the letter of the law. Uncontroverted admissions by NSA officials and their whistleblower agent Edward Snowden evidence the illegality of the agency's unconstitutional conduct - so too does the expert testimony of Edward Felten and the affidavits of Plaintiffs.

Plaintiffs have shown jurisdiction and standing and thus the temporary relief which they seek is justiciable. As Plaintiffs' counsel pleaded at oral argument, this Court must respectfully fulfill its Article III, separation of powers role as protector from this tyranny by the executive branch of government, as our Founding Father, drafter of the Declaration of Independence and third president Thomas Jefferson proclaimed: "When the people fear the government, there is tyranny." The Defendant NSA's surveillance programs and actions clearly have caused the populace to live in fear of their government, which through the agency's access to their metadata of cell phone, internet and social communication records, can be coerced, blackmailed and destroyed by the sovereign for whatever reason. To allow this to continue even for one more day without judicial intervention would be to further this tyranny.

Dated: November 26, 2013

Respectfully submitted,

/s/ Larry Klayman

Larry Klayman, Esq.
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 26th day of November, 2013 a true and correct copy of the foregoing Plaintiffs' Supplemental Brief On Jurisdiction And Standing (Civil Action No. 13-cv-851) 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