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-881

PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF THEIR MOTION FOR PRELIMINARY INJUNCTION

I. INTRODUCTION

On June 12, 2013, Plaintiffs filed suit challenging the legality of Defendants' secret and illicit government scheme to systematically gather, intercept and analyze vast quantities of telephonic and online "metadata" of U.S. citizens. For the past decade, the NSA has engaged in illicit surveillance tactics, utilizing custom-built supercomputers, technical trickery, unlawful court orders, behind-the scenes persuasions, and collaborations with major technology companies, in addition to implementing overreaching unlawful surveillance programs to obtain content and metadata on millions of ordinary Americans without individual warrants. *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. On June 5, 2013, based on the disclosures of whistleblower, Edward Snowden, who fled the United States for fear of government reprisal, *The Guardian* publicly revealed a previously classified order directing Verizon to turn over to the NSA millions of phone records, in an article entitled "*NSA collecting phone records of millions of Verizon*

customers daily. Exclusive: Top secret order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama."[1]

Since 2007, the NSA implemented a highly classified, unlawful mass surveillance program, referred to as PRISM, which is an internal computer system that operates through compelled "partnerships" with major internet companies such as Defendants, who provide Internet, email, social networking, and the like to millions of Americans that use these services as a primary means of communication. Compl. ¶¶3, 8; *See also,* James Ball "*NSA stores metadata of millions of web users for up to a year, secret files show,"* The Guardian, (Sept. 30, 2013), www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents. 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. Compl. ¶7.

The data obtained by the NSA through PRISM 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. *Id.;* Compl. ¶7. The Agency 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. Compl. ¶4.

[1] In the days after *The Guardian* disclosed the Verizon Order, the Director of National Intelligence, James Clapper, acknowledged its authenticity and issued a statement indicating that the FISC had renewed it. *See* Office of the Dir. Of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosure of Classified Information* (June 6, 2013), http://1.usa.gov/13jwuFc. *See also*, Office of the Dir. Of Nat'l Intelligence, *Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata* (July 19, 2013), http://1.usa.gov/12ThY1T.

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 Defendants. Compl. ¶¶8, 9. PRISM, in conjunction with Defendants' illegal participation, has provided the NSA with blanket access to Defendants' vast databases, which contain private electronic records of most, if not all, of the online communications and Internet activities conducted through Defendants' myriad of Internet services and operations. Compl. ¶8. The public disclosure of PRISM has revealed, convincingly, that the communication records of U.S. citizens are being collected indiscriminately and in bulk-regardless of whether they are persons of interests. Compl. ¶52.

The NSA's PRISM program, and Defendant's illegal collaboration with the U.S government, implicates the privacy interests of all users of Defendants' online services, including Plaintiffs' privacy interests. 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. "[A]wareness 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).

Generalized surveillance of this kind has historically been associated with authoritarian and totalitarian regimes, not with constitutional democracies. *See, e.g., United States v. Gordon*, 236 F.2d 916, 919 (2d Cir. 1956); Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1934 (2013) (Until recently, "the threat of constant surveillance has been relegated to the realms of science fiction and failed totalitarian states."). As Jameel Jaffeer, the ACLU's deputy legal director, aptly stated "[I]t is beyond Orwellian, and it provides further evidence of

the extent to which basic democratic rights are being surrendered in secret to the demands of unaccountable intelligence agencies." Compl. ¶36. Such unlawful surveillance schemes by Defendants have subjected untold number of innocent people to the constant surveillance of government agents, invasively intruding, without cause, into the private lives of individuals. At a time when Americans' grievances are not being heard, but are blatantly being ignored by the government, the government has willfully implemented these surveillance tactics as an intimidating and coercive method to ensure that Americans remain submissive. After all, had our Founding Fathers been subjected to such surveillance, they would have been arrested, imprisoned, and executed by King George III and never have made it to Philadelphia to debate and declare independence in 1776.

Defendants, in colluding with Defendant NSA, continue to covertly wage a long-running, highly secretive war against the fundamental constitutional rights of "We The People," through ongoing warrantless surveillance of millions of ordinary Americans. Defendants' "astounding assault on the constitution" has necessitated this lawsuit to stop Defendants' ongoing illegal conduct, which has deprived millions of U.S. citizens, including Plaintiffs, of their fundamental constitutional rights under the First, Fourth, and Fifth Amendments of the U.S. Constitution, intentionally infringing on their rights of privacy, freedom of speech, freedom of association, and the due process. Compl. ¶51. Plaintiffs, therefore, seek a preliminary injunction (1) enjoining Defendants from continuing their unlawful mass surveillance program, and barring Defendants from collecting records pertaining to Plaintiffs' online communications and internet activities under the surveillance program, particularly during the pendency of this case; (2) requiring Defendants to purge from their possession all of Plaintiffs' metadata, including any and all records accessible by the U.S. government and its agencies; and (3) prohibit query of metadata

obtained through the program using any identifier associated with them. Plaintiffs also request an evidentiary hearing and an opportunity to conduct discovery, as the necessary facts, information, documents, and evidence are uniquely in the hands of Defendants. The whistleblower behind the NSA surveillance revelation, Edward Snowden, (who disclosed classified details of several top secret U.S. mass surveillance programs to the press) is currently exiled from the United States but is subject to being deposed under letters rogatories. Other witnesses at the NSA are also subject to discovery. Glenn Greenwald, Ewen MacAskill and Laura Poitras, "*Edward Snowden: the whistleblower behind the NSA surveillance revelations,*" The Guardian (June 10, 2013). http://www.theguardian.com/world/edward-snowden.

Plaintiffs are substantially likely to succeed on the merits of their claims and will suffer irreparable injury if preliminary relief is not granted. Specifically, PRISM is seemingly based on Section 215 of the Patriot Act but disregards the statute's requirements, including its "relevance" requirement. In addition, such warrantless, overreaching, and unreasonable surveillance violates the Fourth Amendment. PRISM also violates the First Amendment because it substantially and unjustifiably burdens Plaintiffs' associational rights, as narrower methods are available for Defendants to achieve their objectives. Indeed, the mass surveillance program at issue is one of the largest surveillance operations ever implemented by the government against its own citizens, and has not only significantly undermined the privacy rights of millions of Americans but has violated their fundamental rights under the U.S. Constitution.

II.
STATEMENT OF FACTS

A. Foreign Intelligence Surveillance Act ("FISA")

In enacting FISA to regulate government surveillance conducted for foreign-intelligence purposes, Congress also created the Foreign Intelligence Surveillance Court ("FISC") and

empowered it to grant or deny government applications for surveillance orders in foreign-intelligence investigations. See 50 U.S.C. §1803(a). Over time, several acts and successor bills, including the Patriot Act, modified the provisions provided under FISA in several respects. In its current form, the statute (now referred to as Section 215) allows the government 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, even if constitutional, which is doubtful, does not provide the government 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). Until recently, the public knew little about Defendants' use of Section 215, let alone Defendants' abuse of the statute to unlawfully obtain detailed intimate information regarding ordinary Americans, in violation of the U.S. Constitution and fundamental privacy rights. Notably, in 2011, Senators Ron Wyden and Mark Udall, both of whom sit on the Senate Select Committee on Intelligence, stated publicly that the government had adopted a "secret interpretation" of Section 215, and validly asserted that Americans would be "stunned," "angry" and "alarmed" when they learned of it. 157 Cong. Rec. S3386 (daily ed. May 26, 2011) (statement of Sen. Ron Wyden); 157 Rec. S3389 (daily ed. May 26, 2011) (statement of Sen. Mark Udall).

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 orders, as further detailed below. *See* Judge Bates' 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); *See also,* 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.

Deeply troubling are the number of misleading statements senior officials have made about domestic surveillance and the extent of Defendants' false misrepresentations and blatant lies. 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 his clearly erroneous and untruthful answer.

In March 2009, the FISC learned that NSA analysts were using the phone log database in ways that went beyond what the judges believed to be the practice because of the NSA's repeated misrepresentations in court filings. In 2011, a federal judge, John D. Bates, then serving

[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).

as chief judge on the FISC, issued an 85-page ruling, which sharply rebuked the NSA for repeatedly misleading the court that oversees its surveillance on domestic soil, including a program that is collecting tens of thousands of domestic e-mails and other internet communications of Americans each year. 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). Judge Bates further admonished the NSA for repeatedly violating the requirements and limitations set forth by Court Orders, privacy laws, and the U.S. Constitution, recognizing that, "[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." *Id.; See also,* Charlie Savage and Scott Shane, *"Secret Court Rebuked N.S.A. on Surveillance,*" 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.

Defendants have 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, "The 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 Defendants 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).

Alarmingly, it has recently been discovered that lower officials 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." 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. More concerning, if lower level employees are capable of such misuse of the agency's surveillance power, then imagine what the higher officials are capable of, with access to such surveillance programs.[3]

B. <u>PRISM, The Mass Call-Tracking Surveillance Program, And The Verizon Order</u>

The National Security Agency ("NSA") has for seven years implemented a highly classified surveillance program known as "PRISM," an internal computer system used to manage domestic and foreign intelligence collected from the internet and through other electronic service providers. Compl. ¶3. PRISM, which operates through compelled "partnerships" with major internet companies, allows the NSA to obtain content and metadata of millions of ordinary Americans without individual warrants. *See,* James Ball "*NSA stores metadata of millions of web users for up to a year, secret files show,"* The Guardian, (Sept. 30, 2013). www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents. In addition

[3] Notably, further evidencing the agency's surveillance power and its misuse is the fact that the NSA even went so far as to monitor the phone calls of 35 world leaders, including Germany's Chancellor Angela Merkel's phone, which has led to the "worst spat between the two countries in a decade." "*NSA Monitored Phone Calls of 35 World Leaders*," The Huffington Post (Oct. 24, 2013) http://www.huffingtonpost.com/2013/10/24/nsa-world-leaders_n_4158922.html. Such surveillance has also involved France, Mexico, and Brazil, as well as other countries. "*Report says NSA monitored 35 world leaders, on heel of Merkel spying claim,"* Fox News (Oct. 25, 2013).

to employing the PRISM program, the NSA has engaged in illicit surveillance tactics, utilizing custom-built supercomputers, technical trickery, unlawful court orders, behind-the scenes persuasions, and collaborations with major technology companies, in addition to implementing overreaching surveillance programs to obtain content and metadata on millions of ordinary Americans without individual warrants. *Id.; S ee* 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.

On June 6, 2013, a mere one day after *The Guardian* had publicly revealed a previously undisclosed unlawful court order directing Verizon Telecommunications to turn over to the NSA the telephone records of over one hundred million Americans on an ongoing daily basis,[4] *The Washington Post* and *The Guardian* obtained a leaked 41-slide security presentation that evidenced the existence of a highly classified surveillance program referred to as "PRISM." *See* "*Here's everything we need to know about PRISM to date*," The Washington Post, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date. Prior to this disclosure, Plaintiffs had no reasonable opportunity to discover the existence of the surveillance program, or its clear violations of statutory and constitutional protection. Compl. ¶6. These publications provided, for the first time, a glimpse into the extent of the NSA's overreaching surveillance tactics and its indiscriminate and in bulk collection of the

[4] Specifically, on April 25, 2013, Defendant Judge Roger Vinson unlawfully ordered Verizon's custodian of records to produce, and to continue production on an ***ongoing daily basis*** **thereafter,** the following tangible things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., to the NSA: all call detail records or "telephony metadata" created by Verizon for communication (i) between the United States and abroad; or (ii) wholly within the United States, including local calls. *In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Serv., Inc. on Behalf of MCI Commc'n Serv., Inc. D/B/A Verizon Bus. Serv.*, Dkt. No. BR 13-80 at 1-2 (FISA Ct. Apr. 25, 2013) (hereinafter "Verizon Order"). "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." *See* Verizon Order.

communication records of over one hundred million U.S. citizens, regardless of whether there is even a hint of reasonable suspicion or probable cause.

PRISM-which operates through compelled "partnerships" with major internet companies-allows the NSA and the Federal Bureau of Investigation ("FBI") to directly access, and collect private electronic data from the central servers of leading U.S. Internet companies, including Google, Facebook, Microsoft, Yahoo!, Apple, Skype, YouTube, AOL, and PalTalk. *See Id.* "NSA stores metadata of millions of web users for up to a year, secret files show." Compl. ¶7. Through procuring a partnership with Defendants, who are the leading Internet service companies, providing Internet, email, social networking, and the like to millions of Americans, the NSA has direct access to the private communications and internet data belonging to the users of Defendants' internet services. More significantly, the NSA is able to extract private audio and video chats, photographs, e-mails, documents and connection logs, by directly accessing Defendants' central servers. *See* Barton Gellman and Laura Poitras, "*U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*," The Washington Post, (June 6, 2013) http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers; Compl. ¶8.

Defendants also manage some of the largest databases in the world containing records of most or all communications made through their myriad of internet services and operations. Compl. ¶8. Defendants have effectively opened their key communication databases to direct and unfettered access by the NSA, disclosing to the government the contents of its users as well as detailed communications of millions of its subscribers and users. Compl. ¶9. More significantly, millions of Americans use Defendants' services as a primary means of communication, all of which has been subject to the NSA's surveillance. Compl. ¶8.

The data obtained by the NSA through PRISM 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. Compl. ¶7. The records obtained by the government contain far more than mere insipid statistical facts. In fact, "…analysis of … metadata often reveals information that could be traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content." Decl. of Professor Edward Felten at ¶39 (herein after, "Decl. of Felten").[5] The communication records and troves of metadata obtained by PRISM through Defendants' vast databases provide the NSA with rich 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. Compl. ¶9

The NSA's indiscriminate and in bulk collection of the communication records of over three hundred million U.S. citizens, regardless of whether there is even a hint of reasonable suspicion or probable cause of any wrongdoing, has undoubtedly subjected untold numbers of innocent people to the constant surveillance of government agents. Compl. ¶¶52, 54.

C. Collection Of Plaintiffs' Records

Plaintiffs, Larry Klayman, Charles Strange, and Mary Ann Strange 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

[5] Professor Edward Felten is a professor of Computer Science and Public Affairs, as well as Director of the Center for Information Technology Policy at Princeton University. He has also served as a consultant/technology advisor in the field of computer science for numerous companies and has authored numerous books, journal articles, and other publications relating to computer science. Additionally, Professor Felten has testified several times before Congress on computer technology issues. Decl. of Felten at ¶¶ 3, 5, 6.

matters and privileged information. Specifically, Plaintiff Larry Klayman is an individual and an attorney who is a subscriber and user of many of the services provided by the major internet companies named in this action, including Google, Facebook, Yahoo!, Microsoft, AT&T, YouTube, and Skpe and has been for many years. Aff. of Larry Klayman at ¶3 (hereafter "Klayman Aff.")(Exhibit 1). Plaintiff Klayman is also the founder, chairman and general counsel of Freedom Watch, a public interest organization dedicated to promoting and protecting civil liberties and individual rights. Klayman Aff. at ¶2. Plaintiff Klayman is known for his strong public interests advocacy in furtherance of ethics in government and protections of individual freedoms and liberties. Klayman Aff. at ¶4. Plaintiff Klayman is publicly recognized as a civil and individual rights activists, often pursuing litigation to safeguard constitutional protections and privacy rights. *Id.* Plaintiff Klayman has filed lawsuits against President Obama and has been highly critical of the Obama administration as a whole. Klayman Aff. at ¶8. More significantly, Plaintiff Klayman was not only responsible for filing the first lawsuits in this NSA surveillance case, but an organizer for the growing "Reclaim America Now" movement, to stop the growing train of government abuses and usurpation. *See* www.reclaimamericanow.net; Klayman Aff. at ¶¶6, 8.

Given the NSA's known conduct, and repeated flagrant misuse of its surveillance powers, it is logical to conclude that Plaintiff Klayman is subjected to excessive and intrusive surveillance and monitoring by the NSA. In fact, it is indisputable that Plaintiff Klayman has become the prime target of the NSA, which is now facing high criticism and being subjected to strict scrutiny of their surveillance programs and policies, as a result of Plaintiff Klayman's highly publicized class action lawsuits against the agency. Klayman Aff. at ¶7. As a result, the NSA is undoubtedly engaging in egregious, alarming, and illegal tactics intended to coerce and

to intimidate Plaintiff Klayman into silence, clearly in an effort to impede on Plaintiff Klayman's public advocacy and, more significantly to obstruct Plaintiff Klayman's pursuit of the legal actions brought against the NSA Klayman Aff. at ¶12. Alarmingly, various contacts of Plaintiff Klayman have even received text messages seemingly sent from Plaintiff Klayman's phone number, even though Plaintiff Klayman had never sent said messages, which raises serious concerns as to the extent of Defendants' conduct and surveillance tactics, and, more significantly, the lengths the NSA will go to in order to coerce Plaintiff Klayman into silence. Klayman Aff. at ¶11.

Plaintiff 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 and communications with whistleblowers and other sources of government abuse and corruption. Klayman Aff. at ¶¶5, 10. Defendants' illegal surveillance directly and significantly impacts Plaintiff Klayman's ability to communicate via telephone, email, and otherwise, at a minimum, 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. Further impairing Plaintiff Klayman's ability to practice law and to adequately serve the best interests of his clients and the public, is the NSA access to online metadata, which provides the agency with a record of nearly everything Plaintiff Klayman does online, from browsing history-such as map searches and websites visited-to account details, email activity, and even some account passwords. The NSA

effectively has unlimited access to the research activities conducted by Plaintiff Klayman, particularly in preparation for a litigation, and for purposes that are intricate and private aspects of practicing law and being the chairman of a non-profit organization, Freedom Watch. 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, whistleblowers, 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. Compl. ¶57; Klayman Aff. at ¶10.

Plaintiff Charles Strange is the father of Michael Strange, a Navy SEAL Team VI support personnel who was killed when the helicopter he was in was attacked and shot down by terrorist Taliban jihadists in Afghanistan on August 6, 2011. Aff. of Charles Strange (hereinafter "Strange Aff.") at ¶5 (Exhibit 2). Specifically, Michael was a Cryptologist Technician, Petty Officer 1st Class (Expeditionary Warfare Specialist) and, given his position with the NSA, Michael had access to all of the secret codes of the NSA and knew intimately the policies, procedures, and practices of the NSA. Strange Aff. at ¶¶5, 6, 7. Specifically, on May 2, 2011, members of the Navy SEAL Team VI carried out an operation that resulted in the capture and killing of Osama Bin Laden. Soon thereafter, Vice President Joseph Biden and Leon Panetta, acting on behalf of President Obama and themselves for political purposes, publicly disclosed the fact that SEAL Team VI was responsible for conducting the successful raid on Osama Bin Laden's compound, thereby making members of SEAL Team VI a target for retaliatory attacks from the Taliban and other Islamic Jihadists. Just three months after the successful raid, Taliban jihadists shot down the U.S. Boeing CH-47 Chinook military helicopter in eastern Afghanistan, killing thirty

Americans, including twenty-two Navy SEALS, including Michael Strange, son of Plaintiff Charles Strange. Strange Aff. at ¶9.

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 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 Present 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 call-tracking surveillance program has directly and significantly impacted both 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. *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. 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.

Following the public disclosure of the NSA's surveillance, it has become clear that the NSA has obtained vast amounts of detailed telephonic and electronic information and breached the confidentiality of Plaintiffs privileged and confidential communications. The secret surveillance that the government is performing on Plaintiffs Charles Strange and his wife, Mary Ann Strange, is causing both of them to be afraid of communicating with their family, friends, and others. Plaintiff Charles Strange is in fear of his safety and his family's safety, fearing immediate bodily injury and even death to himself, his family, and his friends. Strange Aff. at ¶18. This has, inevitably, heightened Plaintiff Charles Strange's emotional distress, causing him to feel as if he is on the verge of a nervous breakdown. Strange Aff. at ¶18. Plaintiff Charles Strange is currently undergoing psychological counseling as a result. Strange Aff. at ¶18.

Similarly, Defendants have indisputably also provided the NSA with intrusive and warrantless access to the internet records of Plaintiffs Michael Ferrari and Matthew Garrison. Plaintiffs Ferrari and Garrison are both 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.

III.
ARGUMENT

To obtain injunctive relief, Plaintiffs must 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. PLAINTIFFS ARE LIKELY TO SUCCEED ON THE MERITS

1. Defendants' Acts Are Not Authorized Under Section 215 Of The Patriot Act.

Defendants' surveillance program is ostensibly based on Section 215 of the Patriot Act, which allows the government to obtain an order requiring the 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*** (other than a threat assessment)…to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." (emphasis added) 50 U.S.C. §1860. The NSA's ongoing mass surveillance program far exceeds the authority provided under Section 215 as it indiscriminately seeks records in bulk not presently relevant to any authorized investigation.

In addition to the relevance requirement, the statute further requires that there be *reasonable grounds* to believe that the tangible things sought are relevant to an *authorized investigation* (other than a threat assessment). An authorized investigation requires factual predicate, whereas a threat assessment does not. See Attorney General's Guidelines for Domestic FBI Operations, U.S. Dep't of Justice, 17-18 (2008). "Reasonable grounds" has been often treated as equivalent to "reasonable suspicion." *See, e.g. United States v. Banks*, 540 U.S. 31,36, (2003); *United States v. Henley*, 469 U.S. 221, 227 (1985). Reasonable suspicion requires a showing of "specific and articulable facts, which, taken together with rational inferences from those facts, reasonably warrant" intrusion into a suspect's privacy. *Terry v. Ohio,* 392 U.S. 1, 21 (1968).

Rather than limit its surveillance to a certain group of people that are subjects of an authorized investigation, the government has instead 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, common

sense and logic dictates that 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.

2. Defendants' Overly Broad, Highly Intrusive Surveillance And Collection Of Plaintiffs' Metadata Violates The Fourth Amendment Of The U.S. Constitution.

The Fourth Amendment of the U.S. Constitution guarantees the right of people to be secure in their persons against unreasonable searches and seizures, that warrants shall not be issued but upon probable cause, and that the place of a search must be described with particularity. U.S. Const. Amend. IV.

(i) Defendants' Surveillance of Plaintiffs' Telephonic Communications, Internet Communications, and Internet Activities Constitutes A Search Under The Fourth Amendment.

A Fourth Amendment search occurs when the "government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyollo v. United States,* 533 U.S. 27, 33 (2001). Under this unequivocal definition of the term "search," Defendants' extensive aggregation of metadata from every phone call made and received in the U.S., revealing the most personal and intimate details of every aspect of each individual's life, profession, and relationships, indisputably constitutes a search.

Plaintiffs, and any other individual in the United States, have a subjective expectation of privacy in their online communications and internet activities. As discussed above, Plaintiffs are particularly vulnerable to this type of surveillance given their professions, political activism, public persons, and their activities, which often involve confidential matters and privileged information. Plaintiffs, and any other individual in the United States communicating online, via

email, chat, or the like, has absolutely no expectation or any reason to expect that the U.S. government has direct access to this private electronic data and is, in fact, collecting, analyzing, and storing such metadata. Nor would Americans expect that their government is using its metadata troves to detail intricate facts regarding individuals' internet communications.

Clearly, Plaintiffs' expectation that their communication records will not be subject to long-term recording, aggregation, and surveillance by the government, is objectively reasonable, particularly as the intrusive surveillance at issue allows the government to gather intricate details of each individual and their associations with one another, including their clients, supporters, and membership. *See United States v. Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). Defendants' conduct clearly constitutes a search under the Fourth Amendment, in which a warrant based on probable cause is required.

(ii) The Government's Scheme and Conduct To Intercept And Analyze Vast Quantities Of Telephonic Communications And Aggregation Of Telephony Metadata Is Unreasonable.

Defendants' surveillance program authorizes 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.

Indeed, Defendants' illegal participation in PRISM and the NSA's mass collection of online 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, the NSA's warrantless surveillance under PRISM is so extreme in its intrusive nature that it can hardly be construed as anything but unreasonable. Specifically, PRISM provides the NSA with direct access to all private electronic data belonging to all users of Defendants' 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 not differentiate between individuals that the government 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.

Moreover, 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 government 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.

3. Defendants' Overly Broad, Highly Intrusive Surveillance And Collection Of Plaintiffs' Metadata Violates The First Amendment Of The U.S. Constitution.

(i) Defendants' Surveillance Tactics Intrudes Upon Private And Confidential Communications, Including Privileged Attorney-Client communications.

As an initial matter, Defendants' illegal participation in PRISM and furthering the NSA's unlawful objective of collecting mass quantities of metadata, compels the production of legally privileged attorney-client communications, which is essential to the "public interest in the observance of law and administration of justice." Specifically, acting under PRISM, Defendants have provided the NSA with direct unfettered access to private electronic data and all communication records, of all users of Defendants' online services, which undoubtedly includes the communication records of Plaintiff Larry Klayman, an attorney and the general counsel of Freedom Watch. At present, Freedom Watch, and consequently, Plaintiff Klayman, is involved in numerous litigations with government agencies, include the litigation with the NSA, the agency primarily responsible for the mass call-tracking surveillance. As a result of PRISM, Defendants effectively turned over Plaintiff Klayman's privileged information to the very parties capable of exploiting that information and using Plaintiffs' communication of legal representations, litigation strategies, and discussions with clients to Defendants' advantage.

In fact, by essentially handing over Plaintiff Klayman's confidential and privileged communications to the NSA, Defendants effectively obstruct Plaintiff Klayman's ability to deliberate, obtain necessary information from his own clients, and develop litigation strategies, "free from the consequences or the apprehension of disclosure." *Hunt v. Blackburn*, 128 U.S.

464, 470 (1888) See also *Weatherford v. Bursey*, 429 U.S. 545, 554, n. 4 (1977) (noting that government surveillance of attorney-client communications threatens the 'inhibition of free exchanges between [client] and counsel."). Thus, Defendants' illicit participation in the PRISM program inevitably allows the NSA to obtain communications protected by attorney-client privilege, and thus, Defendants' conduct should be found unlawful.

(ii) Defendants' Overly Broad, Highly Intrusive Investigative Methods Unnecessarily Impose A Substantial Burden On Plaintiffs' Rights Of Freedom of Speech and Association, While Directly Impeding On The Indispensible Privacy Rights Afforded To Advocacy Groups, Thus Violating Plaintiffs' First Amendment Rights.

The First Amendment provides:

> "Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or of the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. Amend. I.

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 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 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 government's surveillance and investigatory activities infringe on associational rights protected by the amendment. In *Gibson v. Florida Legislative Investigation Committee*, the court ruled, "[t]he First and Fourteenth Amendment rights of free speech and free association are fundamental and highly prized and 'need breathing space to survive." 372 U.S. 539, 892 (1963), citing 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 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 government's broad sweeping surveillance program, particularly under PRISM, 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. PRISM implicitly 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 via email, chat, skype, and the like, with individuals who wish to come forward with evidence of government wrongdoing, such as depriving them of their civil rights. Likewise, Plaintiff Klayman communicates through the internet with not only potential clients but also existing clients, whistleblowers, and other confidential sources of government abuse and corruption to discuss legal matters and advise the clients 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 email, and through other internet communication services, to supporters, potential supporters, members, 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 heard and recorded by the government, particularly as Plaintiffs' advocacy often espouse dissident beliefs than that of the government.

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 government collects and stores every internet communication made through the major online services provided by Defendant under the previously highly classified program, PRISM. Thus, Defendants' participation in the NSA's

overreaching 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. Defendants' Overly Broad, Highly Intrusive Surveillance And Collection Of Plaintiffs' Metadata Violates The Fifth Amendment Of The U.S. Constitution.

The Fifth Amendment provides, in pertinent part, that "No person… shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation." U.S. Const. Amend. V. Pursuant to the Fifth Amendment, Plaintiffs enjoy a liberty interest in their personal security and in being free from the Defendants' and the governments' use of unnecessary and excessive force or intrusion against their persons. Plaintiffs also enjoy a liberty of not being deprived of life, liberty, or property without due process of law. 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.

C. PLAINTIFFS WILL SUFFER IRREPARABLE INJURY IF PRELIMINARY RELIEF IS WITHHELD.

Plaintiffs will suffer irreparable harm absent a preliminary injunction, restraining Defendants from continuing their unlawful surveillance of Plaintiffs especially during this proceeding. Plaintiffs assert injuries resulting from the mass call-tracking surveillance program engaged in by Defendants, which violate Plaintiffs' First, Fourth, and Fifth Amendment rights as well as the program's violation of Section 215 of the Patriot Act. Without a preliminary injunction, Defendants would inherently have a significantly greater and substantially unfair advantage in this lawsuit, especially during the pendency of this action, thus depriving Plaintiffs of their right to a fair trial and rights protected under the First, Fourth, and Fifth Amendments. Courts have consistently held 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 unreasonably been subjected to unconstitutional, warrantless, mass surveillance by PRISM, which was employed by the NSA clearly without proper statutory authority. As explained above, PRISM provides the NSA with indiscriminate access to vast amounts of private electronic data, including records of internet activities and online communications, belonging to users of Defendants' online services. The NSA's unfettered access to mass online metadata through PRISM clearly violates the First, Fourth, and Fifth Amendments of the U.S. Constitution and constitutes an outrageous breach of privacy, freedom of speech, freedom of association, and the due process rights of Plaintiffs and other American citizens. Thus, applying the principles above, a preliminary injunction is proper to prevent further irreparable harm caused by Defendants' participation in PRISM, which implicitly and indisputably resulted in colorable violations of fundamental constitutional provisions.

The PRISM program is particularly illegal, given Plaintiff Klayman's profession as a long-standing attorney advocating for the protection of civil rights and liberties, and the extent of the irreparable harm to Plaintiff Klayman's profession that will result absent a preliminary injunction. Specifically, the NSA's surveillance tactics, and Defendants' unlawful assistance in PRISM, demands production of legally privileged communications between Plaintiff Klayman and current and potential clients regarding their legal representation. Surveillance under PRISM inherently includes the collection of such communication data, in violation of the attorney-client and other privileges and in violation of the confidentiality that attorneys, like Plaintiff Klayman, owe to clients, whistleblowers, and other confidential sources who reveal government abuse and corruption. In light of the above, Defendants should be enjoined until such time as the court can address the very serious constitutional issues raised by Plaintiffs' case.

D. 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. There are already constitutional challenges to the NSA's surveillance programs, including PRISM, both in court and in Congress. Unless and until such challenges are resolved, Defendants should not be permitted to participate in PRISM or further assist the NSA in its highly intrusive surveillance tactic and collection of vast quantities of communication records, particularly where, as here, there are legitimate questions of agency overreach. If the court grants the preliminary injunction, Defendants simply will have to wait until such challenge is resolved before continuing their "partnership" with the NSA and providing the NSA with Plaintiffs private electronic and other data.

E. 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).

IV.
CONCLUSION

For the foregoing reasons, the court should respectfully grant Plaintiffs' motion and enter a preliminary injunction: (1) enjoining Defendants from continuing their unlawful mass surveillance program, and barring Defendants from collecting records pertaining to Plaintiffs' online communications and internet activities under the surveillance program, particularly during the pendency of this case; (2) requiring Defendants to purge from their possession all of Plaintiffs' metadata, including any and all records accessible by the U.S. government and its agencies; and (3) prohibit query of metadata obtained through the program using any identifier associated with them. Plaintiff also requests an evidentiary hearing and an opportunity to conduct discovery, as the necessary facts, information, documents, and evidence are uniquely in the hands of Plaintiffs.

Never before in the history of this nation has a government, aided and abetted by Defendants, so illegally violate the privacy and related interests of its citizens, with the obvious design and intent to coerce and blackmail them into submission to its ends. As Thomas Jefferson, our Founding Father, drafter of the Declaration of Independence, and third American president declared: "When the people fear the government, there is tyranny."

Dated: October 28, 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