IN UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, et. al

Plaintiffs,

v.

BARACK HUSSEIN OBAMA II, et. al

Defendants.

Civil Action No. 13-CV-851

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

I. INTRODUCTION

On June 9, 2013, Plaintiffs filed suit challenging the legality of Defendants' secret and illicit government scheme to systematically gather, intercept and analyze vast quantities of domestic telephonic communications and "metadata" wholly within the United States by implementing a highly classified, unlawful mass call tracking surveillance program. Compl. ¶2.

On April 25, 2013, Defendant Honorable Roger Vinson, a judge of the U.S. Foreign Intelligence Surveillance Court ("FISC"), issued a top-secret order compelling the disclosure of all call detail records in possession of Verizon Telecommunication for analysis by the National Security Agency ("NSA") on an <u>ongoing daily basis</u>.¹ 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 this previously classified order in an article entitled "*NSA collecting phone records of millions of Verizon customers daily. Exclusive: Top secret order*

¹ Compl. ¶26; See, In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs., No. BR 13-80 (FISA Ct. Apr. 25, 2013) ("Verizon Order").

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 2 of 31

requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama.² Compl. ¶2. Prior to this disclosure, Plaintiffs had no reasonable opportunity to discover the existence of this surveillance program or its clear violation of statutory and constitutional protections. Compl. ¶5.

The Guardian's revelation, based on the disclosures of whistleblower Edward Snowden, of the Verizon Order showed, for the first time, that the communication records of U.S. citizens are being collected indiscriminately and in bulk-regardless of whether there is reasonable suspicion or any "probable cause" of any wrongdoing. Compl. ¶31. The FISC and Defendant Vinson far exceeded their statutory authority when issuing this order, and, as such, violated the First, Fourth, and Fifth Amendments of the U.S. Constitution in addition to Section 215 of the Patriot Act. It is the broadest and most illegal surveillance order to have ever been issued, as it outrageously gives the NSA blanket access to the records of all Verizon subscribers anywhere in the United States and overseas, without requiring a hint of reasonable suspicion or probable cause of any wrongdoing. Compl. ¶30. The Verizon Order approved by the FISC violates the privacy interests of all Verizon customers, including Plaintiffs' privacy interests. The records acquired by the NSA under the Verizon Order detail the daily activities, interactions, personal and business relationships, religious and political affiliations, and other intimate details 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

² 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.

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 3 of 31

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 numbers of innocent people to the constant surveillance by 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 would never have made it to Philadelphia to debate and declare independence in 1776.

Defendants 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

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 4 of 31

First, Fourth, and Fifth Amendments of the U.S. Constitution, intentionally infringing on their rights of privacy, freedom of speech, freedom of association, and due process of law. Compl. ¶34. Plaintiffs, therefore, seek a preliminary injunction (1) enjoining Defendants from continuing their unlawful mass call-tracking surveillance program, and barring Defendants from collecting Plaintiffs' call records under this program, particularly during the pendency of this case; (2) requiring Defendants to purge from their possession all of Plaintiffs' call records already collected; and (3) prohibiting Defendants from querying metadata obtained through the program using any phone number or other identifier associated with them, until a permanent injunction can be issued at the end of the case. 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 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. 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. Other witnesses at the NSA are also subject to discovery.

Plaintiffs are substantially likely to succeed on the merits of their claims and will suffer irreparable injury if preliminary relief is not granted. Specifically, the mass call-tracking program is ostensibly based on Section 215 of the Patriot Act but fundamentally disregards the statute's primary requirements, including its "relevance" requirement. Defendants' surveillance violates the Fourth Amendment because the overly broad surveillance carried out is warrantless and unreasonable, and it violates the First Amendment because it substantially and unjustifiably

burdens Plaintiffs' associational rights, as narrower methods are available to Defendants to achieve Defendants' objectives. Indeed, the mass call-tracking surveillance program 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 also illegally 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 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, however, 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 constitutionally protected information regarding ordinary Americans. Notably, in 2011, Senators

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 6 of 31

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 as set forth in court orders. See Nicole Perlott, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," The New York Times (Sept. 5, 2013) http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html. More than 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. These officials have engaged in obstruction of justice, with impunity. The National Intelligence Director, James Clapper, testified before Congress earlier this year that the NSA does not collect data on millions of Americans, which he now admits is a "clearly erroneous" lie. Clapper was asked during a hearing in March by Sen. Ron Wyden if the NSA gathered "any type at all on millions or hundreds of millions of Americans."³ 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

³ See, "*Clapper apologizes for 'erroneous' answer on NSA*." http://news.yahoo.com/clapperapologizes-erroneous-answer-nsa-221238030.html (summarizing Clapper's misleading statements to Congress on the extent of U.S. surveillance on U.S. Citizens).

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 7 of 31

the truth, as evidenced by the public disclosures of a highly classified "Verizon Order" in addition to Clapper subsequently apologizing for, and thus admitted, his clearly erroneous and untruthful answer.

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, the Honorable John D. Bates, then serving as chief judge on the FISC, admonished the NSA for repeatedly violating the requirements and limitations set forth by Court Orders, privacy laws, and the U.S. Constitution. As Judge Bates emphasized, "[c]ontrary to the government's repeated assurances, N.S.A. has been routinely running queries of the metadata using querying terms that did not meet the standard for querying," and that this requirement had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall…regime has never functioned effectively." Charlie Savage and Scott Shane, "Secret Court Rebuked N.S.A. on Surveillance," The New York Times, (Aug. 21, 2013). http://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html?r=0. Judge Bates further emphasized the NSA's unlawful conduct and egregious and illicit surveillance tactics, by stating:

"The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program. In March, 2009, the Court concluded that it s authorization of NSA's bulk acquisition of telephone call detail records from [redacted] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions..."

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

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 8 of 31

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, "[t]he Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information." Amended Memorandum Opinion, *In Re Application of the Federal Bureau of Investigation For An Order Requiring the Production Of Tangible Things From [Redacted]*, (FISC Ct. Aug. 29, 2013) at n.9.

Similarly, in an order issued by the FISC on March 2, 2013, questioning the credibility, trustworthiness, and ability for 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 NSA personnel have been blatantly misusing the NSA's surveillance power to spy on their paramours. NSA Inspector General George Ellard admitted that since 2003, there have been "12 substantiated instances of

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 9 of 31

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.⁴

B. The Mass Call-Tracking Program And The Verizon Order

Since at least 2001, the NSA began a classified surveillance program to intercept the telephone communications of persons within the U.S., a program that continues to this date. Through a top-secret court order, the NSA obtained from Verizon Business Network Services, Inc. "telephony metadata" of all domestic phone calls on the company's network. Compl. ¶¶2, 26. Specifically, on April 25, 2013, Defendant Judge Roger Vinson unlawfully ordered the 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*

⁴ 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).

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 10 of 31

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"). Compl. ¶¶ 26, 27.

"Telephony metadata includes comprehensive communications routing information, including, but not limited to, session identifying information (e.g. originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifiers, telephone calling card numbers, and time and duration of call." Compl. ¶¶27, 28. The "call detail records" referred to in the Verizon Order likely include "[a]ny information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of any call." 47 C.F.R. §64.2003 (2012) (defining "call detail information"). Defendant Vinson further ordered that no person shall disclose to any other person that the FBI or NSA had sought or had obtained tangible things under his order, clearly in an attempt to keep his illegal acts and those of the other Defendants a secret. Compl. ¶29.

Verizon Communications provides services over "America's most advanced fiber-optic network" and operates "America's largest 4G wireless network." *Our company*, Verizon (2013).⁵ It operates the "nations largest all-fiber network serving residential and small business customers," handling an "average of 1 billion calls connected per day." *Fact Sheet*, Verizon (2012).⁶ Verizon also manages some of the largest databases in the world containing records of most or all communications made through their myriad of telecommunication services and operations. Compl. ¶6. Thus, Verizon has essentially opened its key telecommunication

⁵ http://about.verizon.com/index.php/about/our-company

⁶http://about.verison.com/themes/site_themes/agile_records/images/uploads/Verizon_Corporate_ Fact_Sheet.pdf

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 11 of 31

databases to direct access by the NSA, intercepting and disclosing to the government the contents of its customers as well as detailed communications of over one hundred million of its subscribers and users. Compl. ¶7.

The records obtained by the government contain far more than mere insipid statistical facts regarding phone usage data or the length and location of a conversation. In fact, telephony metadata can be extremely revealing, in regard to the individual calls and in the aggregate. Decl. of Professor Edward W. Felten ("Decl. of Felten") at ¶38.⁷ "Although this metadata might, on first impression, seem to be little more than 'information concerning the numbers dialed,' analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content." Decl. of Felten at ¶39.

The communication records and metadata obtained through Verizon provide Defendants with a rich comprehensive profile of every citizen, including an individual's associations, speech, and public movements, in addition to revealing an individual's personal and intimate details about their familial, political, professional, religious, and personal associations. The metadata collected also reveals extremely sensitive information about the caller, including support hotlines for victims of domestic violence and rape, numerous hotlines for people considering suicide, including specific services for first responders, veterans, and teenagers, as well as hotlines for those who suffer from various forms of addiction, such as alcohol, drugs, and gambling. Decl. of Felton at ¶40.

⁷ 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 the U.S. Congress on computer technology issues. Decl. of Felten at ¶¶ 3, 5, 6.

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 12 of 31

Prior to this disclosure, Plaintiffs had no reasonable opportunity to discover the existence of the surveillance program or the severity of Defendants' violations of law and the U.S. Constitution. Compl. ¶5. In fact, Defendant Vinson's Order is the broadest and most illegal surveillance order to ever been issued, allowing the government to collect, indiscriminately and in bulk, the communication records of over one hundred million U.S. citizens, regardless of whether there is even a hint of reasonable suspicion or probable cause of any wrongdoing. Compl. ¶¶30, 31.

B. Collection Of Plaintiffs' Call 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 matters and privileged information. Specifically, Plaintiff Larry Klayman is an attorney who has been a subscriber and user of Verizon Wireless, for many years. Compl. ¶9; Aff. of Larry Klayman at ¶3 (hereafter "Klayman Aff."). 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

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 13 of 31

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. Klayman Aff. at ¶7. 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. Klayman Aff. at ¶15,

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 14 of 31

10. Defendants' illegal surveillance directly and significantly impacts Plaintiff Klayman's ability to communicate via telephone, email, and otherwise, out of fear that his confidential, private, and often legally privileged communications will be overheard or obtained by the NSA's surveillance program. Klayman Aff. at ¶¶9, 10. Defendants' overly broad, highly intrusive illicit surveillance program, as well as their limitless indiscriminate invasion of Americans' privacy rights, undoubtedly will dissuade, and has dissuaded, potential clients and others from contacting Plaintiff Klayman, fearing reprisal, and, in addition, compromises Plaintiff Klayman's ability to serve their clients' interest and Freedom Watch's organizational goals. Klayman Aff. at ¶10.

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

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 15 of 31

Americans, including twenty-two Navy SEALs and support personnel, including Michael Strange, son of Plaintiff Charles Strange. Strange Aff. at ¶9.

Plaintiffs have been vocal about their criticism of President Obama as commander-inchief, his administration, and the U.S. military, particularly in regard to the circumstances surrounding the shoot down of the helicopter Michael Strange was in, which resulted in the death of Michael and other Navy SEAL Team VI and other special operations members. Strange Aff. at ¶¶9, 10. Plaintiffs hold press conferences and lobby in Washington, D.C. as advocates for their son and to obtain justice for him, as well as to change the policies and orders of 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 orchestrated by Defendant NSA and the

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 16 of 31

other Defendants. *Id.* In July of 2013, Mary Ann Strange was on the computer when it abruptly photographed her (through some form of abusive surveillance since her computer does not have a built-in camera), and falsely accused Plaintiff Mary Ann Strange of violating "Copyright and Related Rights Law." Strange Aff. at ¶17. Without a built-in camera, a computer user cannot take a picture of him or herself. Strange Aff. at ¶17. The intrusive and highly secretive surveillance that the government is performing on Plaintiffs has, justifiably, made them unable to communicate freely with friends, family, and other contacts, whether on the phone, through texts messages, or via email and put them in great for themselves and their family. Strange Aff. at ¶18, 19. The government's surveillance activities have, consequently, chilled Plaintiffs' speech, and prohibited their ability to associate, to lobby Congress, and to be politically active. Strange Aff. at ¶18, 19, 20.

Following the public disclosure of the Verizon Order, it has become clear that the NSA has obtained vast amounts of call detail information and breached the confidentiality of their 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.

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, an 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. <u>PLAINTIFFS ARE LIKELY TO SUCCEED ON THE MERITS</u>

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 <u>reasonable grounds</u> to believe that the tangible things sought are <u>relevant</u> to an <u>authorized investigation</u> (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. Defendants further exceed the authority set forth in the statute, by attempting to obtain records not yet in existence, blatantly undermining the statutory purpose behind the provision.

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 18 of 31

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 instead collected "metadata" about every phone call made or received by every resident of U.S. through its boundless and expansive surveillance programs. It is simply inconceivable to conclude that <u>all</u> communication records for <u>all</u> Verizon customers in the United States 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 dictate that the vast majority of Verizon's customers' 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' call records was a warranted and justified intrusion on privacy rights.

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

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

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) <u>Defendants' Surveillance of Plaintiffs' Telephonic Communications, Internet</u> <u>Communications, and Internet Activities Constitutes A Search Under The</u> <u>Fourth Amendment.</u>

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

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 20 of 31

personal and intimate details of every aspect of each individual's life, profession, and relationships, indisputably constitutes a search.

Plaintiffs have a subjective expectation of privacy in their telephone communications and, as discussed above, Plaintiffs are particularly vulnerable to this type of surveillance given their professions, political activism, public personas, and their activities, which often involve confidential matters and privileged information. Plaintiffs, and any other individual in the United States, making and/or receiving a telephone call has absolutely no expectation or any reason to expect that the U.S. government has, in fact, tracked, intercepted, and is gathering metadata regarding the communication. Nor would Americans expect that their government is using its metadata troves to detail intricate facts regarding the phone calls, such as every time the individual picked up the phone, the identity of the person that was called, the precise time the call was made, and how long the conversation lasted.

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) <u>The Government's Scheme To Intercept And Analyze Vast Quantities Of</u> <u>Telephonic Communications And Aggregation Of Telephony Metadata Is</u> <u>Unreasonable.</u>

Defendants' surveillance program authorizes warrantless searches, which "are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 21 of 31

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' collection of metadata and surveillance of telephonic communications lacks any indicia of reasonableness, as it significantly invades Plaintiffs' privacy rights without any probable cause or individualized suspicion, is essentially indefinite, lacks any measure of particularity, instead gathering vast quantities of information about essentially every individual's communication and activities. In fact, Defendant's warrantless surveillance is so extreme in its intrusive nature that it can hardly be construed as anything but unreasonable. Specifically, the Verizon Order requires the production of every communication record, with no attempt to narrow the records obtained to those records that pertain to an ongoing

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 22 of 31

investigation or that have some indication of suspicious activity. The Verizon Order does 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 mass call-tracking program is essentially indefinite, particularly considering the lack of any temporal limitation and the plain language of the Verizon Order. Specifically, the Verizon Order mandates production of communication records on an ongoing daily basis, with no temporal deadline as the Verizon Order is subject to constant renewal. In fact, the government has conducted such overreaching intrusive surveillance for the past seven years, exhibiting no intention of ceasing such conduct. 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. <u>Defendants' Overly Broad, Highly Intrusive Surveillance And Collection Of</u> <u>Plaintiffs' Metadata Violates The First Amendment Of The U.S. Constitution.</u>

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

As an initial matter, the Verizon Order obtained by Defendants 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, the Verizon Order compelled Verizon to turn over to the NSA the communication records of all Verizon users and subscribers, which undoubtedly included 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, including the

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 23 of 31

litigation with the NSA, the agency primarily responsible for the mass call-tracking surveillance. As a result of the Verizon Order, Verizon was required to turn 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, the Verizon Order effectively obstructs Plaintiff Klayman's ability to deliberate, obtain necessary information from his own clients, whistleblowers, and others, 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' boundless orders inevitably sweeps up communications protected by attorney-client and other privilege and privacy interests, and thus, unlawful.

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

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"

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 24 of 31

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 Supreme Court wrote, in explaining why the protection of privacy is of particular Constitutional concern for advocacy organizations:

"[I]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute an effective restraint on freedom of association as the forms of governmental actions....were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's association...Inviolability of privacy in group association may in many

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 25 of 31

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

In light of his public advocacy in matters of public interests and concern, Plaintiff Klayman regularly communicates with individuals who wish to come forward with evidence of government wrongdoing, such as depriving them of their civil rights. Likewise, Plaintiff Klayman communicates with these individuals, who may ultimately become clients, regarding potential legal representation and brining a legal action to redress their harm. Plaintiff Klayman also regularly engages in telephone calls with clients he is already representing, where he discusses legal matters and advises the client, whistleblowers, and others regarding legal strategies and techniques. Similarly, Plaintiffs Charles and Mary Ann Strange, who are activists in advocating change in U.S. military policies and practices, routinely communicate, via phone to clients, potential clients, supporters, and others, regarding the advocacy plans, tactics, strategies and goals. Given the nature of their advocacy, and their inherent affects on government policy and acts, Plaintiffs' communication records contain confidential and even legallyprivileged discussions that were never intended to be collected, monitored, or 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 receives and records every telephone call through this surveillance program. Thus, Defendants' mass call-tracking surveillance program has inevitable had a chilling effect, as it allows the government to uncover anonymous tips or attempts by individuals to privately share sensitive information with Plaintiffs. Consequently, the governments' surveillance program is directly inhibiting and deterring crucial sources of information for Plaintiffs' work.

4. <u>Defendants' Overly Broad, Highly Intrusive Surveillance And Collection Of</u> <u>Plaintiffs' Metadata Violates The Fifth Amendment Of The U.S. Constitution.</u>

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 telephone communications information, 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 is protected by numerous state and federal laws relating to the privacy of communication records as well as the substantive and procedural right to due process

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 27 of 31

under the Fifth Amendment. Defendants clearly violated Plaintiffs' Fifth Amendment constitutional rights the moment they caused Defendant Vinson's order to be illegally granted, thereby giving the government unlimited authority to obtain vast quantities of communication records, including those of Plaintiffs.

Defendants secretly collected, acquired, retained, searched, and used the bulk telephone communication information of Plaintiffs, without providing any notice to Plaintiffs, or process by which Plaintiffs could seek redress. Moreover, Defendants' 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* June 5, 2013 article and Edward Snowden's revelations, 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. <u>PLAINTIFFS WILL SUFFER IRREPARABLE INJURY IF PRELIMINARY</u> <u>RELIEF IS WITHHELD.</u>

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.

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 28 of 31

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 are subjected to ongoing, intrusive, and unlawful surveillance as a result of the mass call tracking surveillance program implemented by Defendants, who do not have the proper statutory authority to engage in such unconstitutional, warrantless, mass surveillance tactics. As explained above, the Verizon Order obtained by the NSA, providing the NSA with indiscriminate access to over one hundred million phone records on a daily basis, 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' mass surveillance program, which constitutes colorable and substantial violations of fundamental constitutional provisions.

Defendants mass call tracking surveillance program is particularly troubling, 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, Defendants' surveillance tactics demand production of legally privileged communications between Plaintiff Klayman and current and potential clients, whistleblowers, and others regarding their legal and other forms of

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 29 of 31

representation. Defendants' surveillance program inherently includes the collection of such communication data, in violation of the attorney-client or other privileges and in violation of the confidentiality that attorneys (including Plaintiff Klayman) owe to clients, whistleblowers, and others with whom they communicate.

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. <u>ISSUANCE OF A PRELIMINARY INJUNCTION WILL NOT SUBSTANTIALLY</u> <u>INJURE DEFENDANTS</u>

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. Defendants are already defending against constitutional challenges to its mass call tracking surveillance program, both in court and in Congress. Unless and until such challenges are resolved, Defendants should not be permitted to continue 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 any surveillance of Plaintiffs.

E. <u>THE BALANCE OF HARM AND THE PUBLIC INTEREST SUPPORTS THE</u> <u>IMPLEMENTATION OF A PRELIMINARY INJUNCTION.</u>

The public interest prong is 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' fundamental defects in complying with court orders and their substantially likely constitutional violations, the public interest will be served if this court preliminarily enjoins Defendants from continuing their warrantless, unlawful surveillance. In light of the fact that Defendants' mass call tracking surveillance program poses legitimate and unaddressed constitutional questions, a preliminary injunction to allow for the evaluation of such questions 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 that, during the pendency of this suit, (i) bar Defendants from collecting Plaintiffs' call records under the mass call surveillance program; (ii) require Defendants to destroy all of Plaintiffs' call records already collected under the program; and (iii) prohibit

Case 1:13-cv-00851-RJL Document 13-1 Filed 10/29/13 Page 31 of 31

Defendants from querying metadata obtained through the program using any phone number or other identifier associated with Plaintiffs. Plaintiffs further respectfully requests an evidentiary hearing and an opportunity to conduct discovery, as the facts, information, documents, and evidence are uniquely in the hands of Defendants.

Never before in the history of this nation has a government, aided and abetted by Defendants, so illegally violated 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