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 and Civil Action No. 13-CV-851

[PROPOSED] MEMORANDUM OPINION AND ORDER GRANTING PLAINTIFFS' MOTIONS FOR PRELIMINARY INJUNCTION

Plaintiff, Larry Klayman, ("Klayman"), a former U.S. Department of Justice prosecutor, Plaintiff Michael Ferrari, ("Ferrari"), Plaintiff Charles Strange, ("Strange"), and Plaintiff Matt Garrison, ("Garrison"), (collectively "Plaintiffs"), have moved for a preliminary injunction, pursuant to Federal Rule of Civil Procedure ("FRCP") 65, to enjoin the National Security Agency ("NSA" or "Defendants") from continuing their illegal mass warrantless surveillance of ordinary Americans without reasonable suspicion or probable cause and to order Defendants to comply with statutory and constitutional laws.

Having considered the motion, the opposition thereto, the record of the case, and the argument of counsel at the hearing, the Court finds that Plaintiffs have demonstrated a substantial likelihood of succeeding on the merits, that they are likely to suffer irreparable harm without a preliminary injunction, that a preliminary injunction would not substantially injure the other parties, and that the public interest would be furthered by granting the order. Accordingly, the Court GRANTS Plaintiffs' Motion for a preliminary injunction enjoining Defendants from exceeding statutory and constitutional authority and further ORDERS Defendants to comply with any and all applicable laws.

I.
JURISDICTION

1. This Court has jurisdiction over the subject matter of this case and it has jurisdiction over all the parties hereto pursuant to 28 U.S.C. §1331. 28 U.S.C. §1331 states, in pertinent part, "[t]he district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States." Venue is proper under 28 U.S.C. §1391.

2. This Court has supplemental jurisdiction pursuant to 28 U.S.C. §1367, which states in pertinent part, "…in any civil action of which the district courts have original jurisdiction, the district courts shall have supplemental jurisdiction over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the U.S. Constitution. Additionally, this Court has authority to grant a preliminary injunction and other appropriate relief pursuant to FRCP Rule 65.

II.
STANDING

3. Plaintiffs have standing under Article III. They have suffered an injury because they are U.S. citizens who have, at all material times, been subscribers, users, customers, and otherwise have availed themselves to Verizon, Facebook, Yahoo, Google, Microsoft, YouTube, AOL, PalTalk, Skype, Sprint, AT&T, and/or Apple. PRISM Compl. ¶ 1; Verizon Compl. ¶ 1. Plaintiffs' communications have been, and continue to be, monitored by Defendants under the Verizon Order and/or Defendants' PRISM surveillance program PRISM Mot. for Preliminary Injunction at 4 (hereafter "Mot. for PI").

4. The injury is plainly traceable to the conduct they challenge—that is, to Defendants' collection of their call records as well as their internet communications and activities. And the injury would be redressed by the relief they seek—principally, an injunction against their mass warrantless surveillance tactics. The practice is akin to snatching every American's address book—with annotations detailing whom they spoke to, when they talked, for how long, and from where. Verizon Compl. ¶ 28. The collection of Plaintiffs' communication records, specifically telephonic and online metadata belonging to Plaintiffs, is itself an injury sufficient for Article III; indeed, the collection of Plaintiffs' records constitutes a gross invasion of their privacy. PRISM Compl. ¶10.

5. Defendants have acknowledged that it has engaged in such metadata collection. Specifically, in regard to the PRISM surveillance program, Defendants have essentially confirmed the existence of the wide-ranging program known as PRISM, which allows the NSA to directly tap into consumer data from telephone and internet communication service providers, including Apple, Google, Yahoo!, Microsoft, Facebook, Skype, and others. Mot. for PI at 10-11. In addition, the Primary Order/Verizon Order indicates that every time the NSA queries the call-records database, it reviews ***everyone's records***—Plaintiffs' among them—to determine whether they, their contacts, or their contacts' contacts are connected to a phone number that the NSA deems suspicious. See Primary Order at 6–7, 11.

6. In any event, there can be no dispute that the bulk collection of Plaintiffs' communication records gives them the stake in this litigation that Article III requires. Courts frequently analyze third-party challenges to records requests at the merits stage, rather than as a question of standing. See, e.g., *Local 1814, Int'l Longshoremen's Ass'n v. Waterfront*

Comm'n of N.Y. Harbor, 667 F.2d 267, 270 (2d Cir. 1981). Plaintiffs' First Amendment claim asserts a direct intrusion into their associational privacy, not just a chilling effect. PRISM Compl. ¶ 76-78.

7. This intrusion and the resulting injury is complete when Defendants collect Plaintiffs' communication records—regardless whether the surveillance ultimately dissuades any third party from communicating with them. Additionally, Plaintiffs suffer a further, discrete injury because of the program's chilling effect on their key contacts and sources. As way of example, Plaintiff Larry Klayman is an attorney and, more significantly, is the founder, chairman, and general counsel of Freedom Watch, an organization devoted to promoting and preserving civil liberties and individual rights. Mot. for PI at 13-19. As an attorney, Plaintiff Klayman routinely communicates by phone and by email with existing and potential clients about their legal representation, discusses confidential issues, and engages in legally privileged attorney-client and other privileged or private communications regarding ongoing legal proceedings. Klayman Aff. at ¶¶5, 10. Defendants' illegal surveillance directly and significantly impacts Plaintiff Klayman's ability to communicate via telephone, email, and otherwise, out of fear that his confidential, private, and often legally privileged communications will be overheard or obtained by the NSA's surveillance program. Klayman Aff. at ¶¶9, 10. Defendants' overly broad, highly intrusive illicit surveillance program has and will continue to dissuade, potential clients and others from contacting Plaintiff Klayman, fearing reprisal, and, additionally, compromises Plaintiff Klayman's ability to serve their clients' interest and Freedom Watch's organizational goals. Klayman Aff. at ¶10. With public knowledge and wide disclosure of the NSA's surveillance, the NSA's monitoring has and will

continue to dissuade crucial contacts from associating with Plaintiff. *Id.* Because he now fears that his telephone conversations and emails are being monitored -- because they are -- Plaintiff Klayman no longer engages in sensitive attorney-client conversations over the phone or by email. Supplemental Klayman Aff. at ¶13. Plaintiff Klayman has been forced to travel to meet with clients in order to ensure that his conversations are indeed private. Supplemental Klayman Aff. at ¶14. This constant travel has come as a great expense to Plaintiff Klayman. *Id.*

8. The NSA seems to believe that there is something implausible about the notion that the NSA's surveillance might chill lawful expression and association, but "[i]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective . . . restraint on freedom of association." *NAACP v. Alabama*, 357 U.S. 449, 462 (1958); *Talley v. California*, 362 U.S. 60, 64 (1960).

III.
FINDINGS OF FACT

9. Pending before this Court are two separate lawsuits filed by Plaintiffs, challenging the constitutionality of the NSA's actions of engaging in mass warrantless domestic surveillance tactics, which illicitly gathered the communication records of hundreds of millions of U.S. citizens.

10. Plaintiffs' lawsuits arose when NSA whistleblower, Edward Snowden, publicly revealed, during an interview with journalist Glenn Greenwald of The Guardian, the NSA's secretive mass domestic surveillance of U.S. citizens, and the existence of the surveillance program commonly referred to as "PRISM." *See*, Tr. of Edward Snowden Interview with The Guardian (hereafter "Tr. of Snowden"); Glen Greenwald, "*XKeyscore: NSA tool collects 'nearly everything a user does on the internet*'," The

Guardian (July 31, 2013). http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

11. Snowden worked as an infrastructure analyst for the NSA in Hawaii and had previously held numerous positions within the intelligence community, including positions as a senior adviser for the Central Intelligence Agency, solutions consultant, and a telecommunications information system officer. Tr. of Snowden at Pg. 1. As an agent of the NSA, Snowden was exposed to, and had access to, privileged information regarding the intelligence community agencies and their course of conduct. *Id.*

12. During the interview with The Guardian, Snowden made the following pertinent statements regarding the NSA's domestic surveillance, which targeted hundreds of millions of U.S. citizens[1]:

    a. "When you're in positions of privileged access like a systems administrator for the sort of intelligence community agencies, you're exposed to a lot more information on a broader scale then the average employee and because of that you see things that may be disturbing but over the course of a normal person's career you'd only see one or two of these instances. When you see everything you see them on a more frequent basis and you recognize that some of these things are actually abuses…" *See,* Tr. of Snowden at Pg. 1.

    b. "NSA and intelligence community in general is focused on getting intelligence where it can by any means possible." *See* Tr. of Snowden at Pg. 1.

    c. "Now increasingly we see that it's happening domestically and to do that they, the NSA specifically, targets the communications of everyone. It ingests them by default. It collects them in its system and it filters them and it analyzes them and it measures them and it stores them for periods of time… so while they may be

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

intending to target someone associated with a foreign government or someone they suspect of terrorism, they're collecting your communications to do so." *See* Tr. of Snowden at Pg. 1.

d. "Any analyst at any time can target anyone, any selector, anywhere… I sitting at my desk certainly had the authorities to wiretap anyone from you or your accountant to a Federal judge to even the President if I had a personal e-mail." *See,* Tr. of Snowden at Pg. 1.

e. "…Even if you're not doing anything wrong you're being watched and recorded. And the storage capability of these systems increases every year consistently by orders of magnitude to where its getting to the point where you don't have to have done anything wrong…and [the NSA] can use this system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with…" *See,* Tr. of Snowden at Pg. 2.

13. Following Snowden's revelations, and subsequent evidence that came to light, Plaintiffs' filed two lawsuits, challenging the NSA's surveillance tactics.

14. Specifically, on June 9, 2013, Plaintiffs filed an action challenging the legality of an overreaching, highly classified, order issued by the Foreign Intelligence Surveillance Court ("FISC"), which provided the NSA with access to **ALL** communication records from **ALL** subscribers, consumers, and users of Verizon communications, without any reasonable suspicion or probable cause of wrongdoing. *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) (hereafter, "Verizon Order")/

15. On June 12, 2013, Plaintiffs filed a separate suit challenging the legality of Defendants' secret and illicit scheme to systematically gather, intercept and analyze vast quantities of telephonic and online "metadata" of U.S. citizens through the NSA's PRISM program[2], which monitors and intercepts communications from internet companies such as Skype,

[2] Unlike the Verizon Order, the PRISM program was not implemented pursuant to any court order from the FISA court.

Google, Youtube, AOL, Yahoo!, Facebook, Paltalk, AT&T, Sprint, and Microsoft. *See*, PRISM PowerPoint Slides Re: Data Acquisition. (These slides consist of NSA training slides about the acquisition of surveillance information through the PRISM program).[3] The PRISM lawsuit also challenges Defendants' expansive acquisition of Plaintiffs' telephonic and online communication records under Section 215 of the Patriot Act, 50 U.S.C. §1860 through the PRISM surveillance program.

16. On October 29, 2013, Plaintiffs filed, in both cases, a Motion for Preliminary Injunction seeking to enjoin Defendants from continuing their illegal mass warrantless surveillance of ordinary Americans without reasonable suspicion or probable cause and to order Defendants to comply with statutory and constitutional laws. Defendants filed an Opposition to Plaintiffs' Motions for Preliminary Injunctions on November 12, 2013 (despite this Court's Order that the deadline for Defendants to file their Opposition was November 11, 2013). The matter regarding the issuance of a preliminary injunction was set for hearing on November 18, 2013.

(A) The PRISM Surveillance Program

17. 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,*"

[3] Following Plaintiffs' filing of the PRISM action, it has been discovered that the NSA has implemented yet another mass surveillance program, referred to as MUSCULAR. See, NSA: Special Operations Weekly Excerpt (an excerpt from the Special Operations weekly, which is an internal NSA publication describing data collection via the MUSCULAR program.)

The Guardian, (Sept. 30, 2013), www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

18. 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, which not only includes the contents of emails, chats, VoIP calls, and cloud-stored files, and more but also provides the NSA 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. *See, i.e.* HJC Hearing at 29:33–36:00 (testimony of John C. Inglis, NSA Deputy Director).

19. The metadata gathered through PRISM allows the NSA 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.

20. Further, "…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").[4]

21. In fact, programs such as PRISM *were* used to illegally wiretap Chancellor Angela Merkel of Germany. *See* Alison Smale and David E. Sanger, "*Spying Scandal Alters U.S.*

[4] 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.

Ties With Allies and Raises Talk of Policy Shift," The New York Times (November 11, 2013), http://www.nytimes.com/2013/11/12/world/spying-scandal-alters-us-ties-with-allies-and-raises-talk-of-policy-shift.html.

(B) The Verizon Order

22. On April 25, 2013, Defendant Judge Roger Vinson issued a highly classified order directing the Custodian of Records of Verizon Business Network Services, Inc. ("Verizon") to produce, and to continue production on an ***ongoing daily basis*** **thereafter,** the following tangible things 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").

23. "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. 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").

24. Defendants have disclosed that the Verizon Order was issued as part of a broader program that has been in place for seven years and that involves the collection of information about virtually every phone call, domestic and international, made or received in the United States. *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act* 1 (Aug. 9, 2013), http://bit.ly/15ebL9k ("White Paper"); Dep't of Justice, *Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization* 3 (Feb. 2, 2011), http://1.usa.gov/1cdFJ1G.

25. Moreover, the Primary Order and the administration's White Paper explain how Defendants analyze and disseminate information housed in the massive database assembled by the call tracking program. Specifically, the documents indicate that the NSA is permitted to query this database when a "designated approving official" at the NSA determines that "there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with" a "foreign terrorist organization." Primary Order at 7.

26. Defendants have acknowledged that the NSA has violated the Primary Order's restrictions on multiple occasions. White Paper at 5. ("Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues that were discovered as a result of DOJ and ODNI reviews and internal NSA oversight."). White Paper at 5.

(C) NSA's Countless Non-Compliance Incidences with Surveillance Laws and Regulations

27. There have been countless incidences of non-compliance incidents involving the NSA's surveillance. Moreover, 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.

28. A 2012 quarterly audit of the NSA's surveillance activities describes 2,766 violations by the NSA of the surveillance laws and its internal rules and regulations. *See*, "SID Oversight and Compliance Audit."

29. In addition, NSA Inspector General George Ellard admitted that since 2003, there have been "12 substantiated instances of intentional misuse" of "surveillance authorities." *See*, Attached Touhy Letter with Attached Documents Requesting Authentication From the NSA, *(Letter of NSA Inspector General George Ellard to Senator Chuck Grassley.)* About all of these cases involved an NSA employee spying on a girlfriend, boyfriend, or some kind of love interests. Jake Gibson, *"Too tempting? NSA watchdog details how officials spied on love interests,"* FOX News, (Sept. 27, 2013).

30. In 2009, the NSA issued a memo to notify the House Permanent Selection Committee on Intelligence Compliance Incidents identified under the ongoing end-to-end review of bulk telephony metadata under Section 215. *See*, "NSA Memo: Congressional Notification and Incidences of Compliance."

31. Evidencing yet another example of the NSA's non-compliance with statutory laws and court orders, an NSA document ("FAA Certification Renewals with Caveats"),

describing the FISA Court's 2011 FAA Certifications, confirms the FISC ruling that certain procedures implemented by the NSA for the collection of "Multiple Communications Transactions" were "deficient on statutory and constitutional grounds." *See*, "FAA Certification Renewals with Caveats."

32. Additionally, a Memorandum Opinion issued by the FISC in October 2011, ruled one of the NSA's communications collection program as unconstitutional. *See*, FISC Memorandum Opinion, dated October 2011.

(D) NSA's Repeated Pattern of Lying Regarding Mass Surveillance, Non-Compliance with Court Orders, and Engaging in Illegal Surveillance Tactics

33. In addition to the reoccurring incidences of non-compliances with U.S. laws and regulations, the NSA has repeatedly engaged in a pattern of lying and deceptive conduct. As such, this Court cannot rely on the statements made by the NSA in their pleadings, given the NSA's pattern of lying to the American people, which raises a strong inference of their continuing deceptive, misleading allegations and contentions.

34. Defendants' deceptive conduct has been evidenced through numerous instances of unlawful actions, 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.

35. 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. In fact, James Clapper, the Director of National Intelligence, lied under

oath during a congressional hearing by denying that the NSA was collecting mass quantities of domestic communication records. *See,* "*Clapper apologizes for 'erroneous' answer on NSA*." http://news.yahoo.com/clapper-apologizes-erroneous-answer-nsa-221238030.html. Specifically, 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."[5] 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." *See,* "*Clapper apologizes for 'erroneous' answer on NSA*." http://news.yahoo.com/clapper-apologizes-erroneous-answer-nsa-221238030.html.

36. Clapper now admits that his testimony is a "clearly erroneous" lie and, in fact, confirmed this in a letter to the Honorable Dianne Feinstein, wherein Clapper admitted that he had lied during the congressional hearing. *See*, "Clapper Letter to Hon. Dianne Feinstein," dated June 21, 2013.

37. Unsurprisingly, the Obama administration has been caught lying in one scandal after another, including but not limited to Obamacare, Benghazi, the IRS, and Fast and Furious, just to name a few.

38. Moreover, the FISC has made numerous findings of repeated violations by the NSA of court orders.

39. The FISC has made findings of repeated violations of court orders. In 2011, the Honorable John D. Bates, then serving as chief judge on the FISC, admonished the NSA

[5] *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).

for repeatedly violating the requirements and limitations set forth by Court Orders, privacy laws, and the U.S. Constitution. 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.

40. 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.

41. 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.

42. In an 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.

43. 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).

IV.
STATUTORY AND REGULATORY BACKGROUND AND FRAMEWORK

44. Defendants' surveillance program is ostensibly based on Section 215 of the Patriot Act, which allows Defendants 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.

45. In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") to regulate government surveillance conducted for foreign-intelligence purposes. Congress adopted FISA after the Supreme Court held, in *United States v. U.S. District Court* (*Keith*), 407 U.S. 297(1972), that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. In enacting FISA, Congress created the Foreign Intelligence Surveillance Court ("FISC") and empowered it to grant or deny government applications for surveillance orders in foreign intelligence investigations. 50 U.S.C. § 1803(a).

46. The provision at issue in this case was originally added to FISA in 1998. *See* 50 U.S.C.§§ 1861–1862 (2000 ed.). The Patriot Act and several successor bills modified that provision in several respects. In its current form, the statute—commonly referred to as Section 215—allows the NSA 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." *Id.* § 1861(b)(2)(A). While the amendments to this provision expanded the government's investigative power, this expansion was not without limits. For example, language added by the Patriot Act prohibits the NSA from using the provision to obtain tangible things that could not be obtained through analogous mechanisms.

V.
CONCLUSIONS OF LAW

Standard for Preliminary Injunctive Relief

47. This Court may issue a preliminary injunction only when the movant demonstrates: (1) a substantial likelihood of success on the merits; (2) that it would suffer irreparable injury if the injunction is not granted; (3) that an injunction would not substantially injure other interested parties; and (4) that the public interest would be furthered by the injunction. *Mova Pharm. Corp. v. Shalala*, 140 F.3d 1060, 1066 (D.C. Cir. 1998) (quoting *CityFed Fin. Corp. v. Office of Thrift Supervision*, 58 F.3d 738, 746 (D.C. Cir. 1995). "These factors interrelate on a sliding scale and must be balanced against each other." *Serono Labs., Inc. v. Shalala*, 158 F.3d 1313, 1318 (D.C. Cir. 1998).

(1) Plaintiffs have Demonstrated a Substantial Likelihood of Success on the Merits

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

unjustifiably burdens Plaintiffs' associational rights when more narrow methods could be used to achieve Defendants' ends.

(2) Plaintiffs Will Suffer Irreparable Harm

49. 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.

50. Additionally, 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 *Serets-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 or constitutional authority to engage in such warrantless, mass surveillance tactics, through obtaining such orders as the Verizon Order and implementing programs such as the PRISM program.

(3) Defendants Will Not be Substantially Harmed by an Issuance of a Preliminary Injunction

51. Defendants cannot be said to be "burdened" by a requirement to comply with the law. 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. Thus, Defendants' will not be substantially harmed by an Order mandating that they comply with the law.

(4) Public Interest

52. 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.") *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).

53. 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.

VI.
CONCLUSION

54. In accordance with the memorandum opinion issued this date, and upon consideration of the Plaintiffs' Motion for a Preliminary Injunction, the opposition thereto, the reply brief, the applicable law, and the arguments made by counsel during the hearing conducted by the Court on this matter, it is hereby ORDERED that the Plaintiffs' Motion for the Preliminary Injunction is GRANTED; and it is further ORDERED that the Court hereby enters the following preliminary injunction.

a. The Court hereby preliminary RESTRAINS AND ENJOINS Defendants, its agents, servants, employees, attorneys, and all others in active concert or participation with Defendants, from implementing surveillance procedures, tactics, and programs that exceed statutory authority and constitutional provisions.

b. Defendants are further ORDERED to comply with any and all laws regarding the Defendants' authority, power, and limits in conducting such mass warrantless domestic surveillance, including, but not limited to, Section 215 of the Patriot Act, Section 702 of the FISA Amendment Act, and the provisions of the U.S. Constitution.

c. It is further ORDERED that within twenty (20) days of this date, Defendants must submit declarations and any pertinent records, reports, and/or other documents to the Court regarding compliance with any and all minimization procedures implemented to prevent further warrantless collection of records belonging to

U.S. citizens without reasonable suspicion or probably cause, any and all incidences of non-compliance, identification of any and all "targets" subject to Defendants' surveillance, and all other relevant reports, risk assessments, memoranda, and other documents. In the event that the records, reports, and/or other documents contain classified information, Defendants shall present such information in camera to the Court.

d. The plaintiffs, in accordance with their discovery rights, may take discovery regarding Defendants' declarations. The Plaintiffs must file any responses to Defendants submissions under this section within thirty (30) days of the completion of the Plaintiffs' discovery. The Court will consider the parties' submissions, conduct any necessary evidentiary hearing, and order further relief as appropriate.

e. It is further ORDERED that proper procedures shall be taken by Plaintiffs' counsel to obtain a security clearance in order to conduct said discovery.[6]

f. It is further ORDERED, in accordance with the Federal Rules of Civil Procedure, that the Plaintiffs' discovery rights are reconfirmed. The Plaintiffs may take discovery, by deposition or otherwise, regarding any pertinent records, reports, and/or other documents to the Court regarding compliance with any and all minimization procedures implemented to prevent further warrantless collection of records belonging to U.S. citizens without reasonable suspicion or probably cause, any and all incidences of non-compliance, identification of any and all "targets" subject to Defendants' surveillance, and all other relevant reports, risk

[6] Plaintiffs' counsel, Larry Klayman, was a former Department of Justice attorney with the anti-trust division and has previously obtained a security clearance.

assessments, memoranda, and other documents. The scope of Plaintiffs' discovery requests may include "all relevant reports, risk assessments, memoranda, and other documents, whether prepared by the National Security Agency officials or employees, officials or employees of other government agencies, or third parties, any pertinent records, reports, and/or other documents to the Court relating to Defendants' compliance with any and all minimization procedures implemented to prevent further warrantless collection of records belonging to U.S. citizens without reasonable suspicion or probably cause, any and all incidences of non-compliance, identification of any and all "targets" subject to Defendants' surveillance, and all other relevant reports, risk assessments, memoranda, and other documents.

g. The parties shall endeavor to agree upon and submit to the Court, within ten (10) days of this date, a proposed protective order to govern disclosure of information and materials related to Defendants' surveillance. In the event that the parties are unable to agree on a proposed protective order, each party must submit a proposed protective order to the Court within ten (10) days of this date.

h. No bond is required. The balance of hardships favors Plaintiffs, who are experiencing harm to fundamental rights guaranteed them by the Constitution, while Defendants do not face a likelihood of financial or other harm from complying with this injunction.

IT IS SO ORDERED

_____

Hon. Richard J. Leon
United States District Judge