

IN THE UNITED STATES DISTRICT COURT FOR
THE DISTRICT OF COLUMBIA

RAND PAUL, on behalf of himself
and all others similarly situated;
P.O. Box 15643
Washington, D.C. 20003

and

FREEDOMWORKS, INC., on behalf of itself, its members,
and all others similarly situated;
400 North Capitol Street, N.W., Suite 765
Washington, D.C. 20001

Civil Action No. _____

Plaintiffs,

v.

BARACK H. OBAMA, in his official capacity as President of the United States;
Office of the President, The White House
1600 Pennsylvania Ave., N.W.
Washington, DC 20500

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence;
Office of the Director of National Intelligence
Attn: James R. Clapper
Washington, D.C. 20511

KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency
and Chief of the Central Security Service;
National Security Agency
Attn: General Keith B. Alexander
9800 Savage Rd.
Fort Meade, MD 20755

and JAMES B. COMEY, JR., in his official capacity as Director of the Federal Bureau of
Investigation;
FBI Headquarters
935 Pennsylvania Avenue,
N.W., Washington, D.C. 20535-0001

Defendants.

Additional service on behalf of Defendants President Obama, Director Clapper and Director Comey:

Ronald C. Machen Jr.
U.S. Attorney for the District of Columbia
Judiciary Center Building
555 Fourth Street, NW
Washington, DC 20530

Additional service on behalf of Defendant General Alexander:

Rod J. Rosenstein
U.S. Attorney for the District of Maryland
6406 Ivy Lane Suite 800
Greenbelt, MD 20770

CLASS ACTION COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Plaintiffs, on behalf of themselves and all other similarly situated United States citizens or permanent residents who are or have been customers, users, or subscribers of phone service in the United States since 2006, bring this action for declaratory and injunctive relief against Defendants' mass, suspicionless, non-particularized collection, storage, retention, and search of telephone metadata related to every domestic or international phone call made or received by Plaintiffs and class members (hereinafter "Mass Associational Tracking Program" or "MATP") under the auspices of Section 215 of the Patriot Act, 50 U.S.C. § 1861, in violation of the Fourth Amendment of the United States Constitution.¹ Plaintiffs and class members seek a declaration that the Mass Associational Tracking Program is unconstitutional, an injunction forbidding the government from continuing the MATP, and an order to the Defendants to purge from its MATP databases all of the telephone metadata related to the communications of Plaintiffs and class members. Plaintiffs and class members aver as follows:

¹ The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

SUBJECT MATTER JURISDICTION AND AUTHORITY TO GRANT RELIEF

1. This Court has subject matter jurisdiction over the Complaint under 28 U.S.C. § 1331 because the claims of Plaintiffs and class members arise under the Constitution of the United States. This Court has authority to grant declaratory relief under the Declaratory Judgment Act, 28 U.S.C. §§ 2201-2202. This Court has authority to award costs and attorney's fees pursuant to 28 U.S.C. § 2412.

PERSONAL JURISDICTION

2. This Court possesses personal jurisdiction over the Defendants because their acts or omissions giving rise to the claims of Plaintiffs and class members occurred in this district or because of their regular or continuous presence or residence in this district.

VENUE

3. Venue is proper under 28 U.S.C. § 1391(e) because a substantial portion of the events or omissions giving rise to the claims of Plaintiffs and class members occurred in this district, and, upon information and belief, one or more of Defendants reside in this district.

PARTIES

PLAINTIFFS

4. Plaintiff and Class Representative Rand Paul is a citizen of the United States and a resident and citizen of Kentucky. Plaintiff Paul has standing to bring this suit because Defendants have, without legitimate legal basis, collected, stored, retained, and periodically searched

telephone metadata concerning every domestic or international phone call he made or received since at least May 2006, and Defendants continue to do so. Plaintiff Paul uses and has used both cellular and/or landline telephones in the United States on a daily basis since May 2006, and he has been a subscriber of both cellular and landline telephone services since May 2006. Such telephone services have included, but not been limited to, Verizon Wireless and AT&T services. Plaintiff has a subjective expectation of privacy from Defendants about his telephone metadata that society views as reasonable.

5. Plaintiff and Class Representative FreedomWorks, Inc. is a not for profit Washington, D.C. corporation ("FreedomWorks"), exempt from taxation under Section 501(c)(4) of the Internal Revenue Code. Plaintiff FreedomWorks has standing to bring this suit because Defendants have, without legitimate legal basis, collected, stored, retained for five years, and periodically searched telephone metadata concerning every domestic or international phone call made or received by FreedomWorks' employees and members since at least May 2006, and Defendants continue to do so.² Plaintiff FreedomWorks's employees and members use both cellular and landline telephones in the United States, and FreedomWorks is a subscriber of both cellular and landline telephone services. FreedomWorks also funds the cellular telephone plans of many of its employees. Such telephone services have included, but not been limited to, Verizon Wireless and AT&T services. Plaintiff FreedomWorks has a subjective expectation of privacy from Defendants of its telephone metadata that society views as reasonable.

² FreedomWorks has approximately 6,000,000 participating members and over 65,000 financially supporting members.

DEFENDANTS

6. Defendant Barack H. Obama is the President of the United States endowed with ultimate authority over each of the federal agencies relevant to this action.
7. Defendant James R. Clapper is the Director of National Intelligence endowed with ultimate authority over the activities of the intelligence community, including activities undertaken pursuant to Section 215 of the Patriot Act, 18 U.S.C. § 1861, and the Mass Associational Tracking Program.
8. Defendant Lt. General Keith Alexander is the Director of the National Security Agency (“NSA”), in the Department of Defense, and is Chief of the Central Security Service. Lt. General Alexander has ultimate authority to supervise and implement all functions and operations of the NSA, the agency that has and continues to conduct the Mass Associational Tracking Program under the auspices of Section 215 of the Patriot Act. Lt. General Alexander personally authorizes and supervises the Mass Associational Tracking Program.
9. Defendant James B. Comey, Jr. is the Director of the FBI and is responsible for applications made to the Foreign Intelligence Surveillance Court for orders demanding the production of “tangible things” under Section 215 of the Patriot Act, which is a cornerstone of the Mass Associational Tracking Program.

STATEMENT OF FACTS

Foreign Intelligence Surveillance Act

10. Congress enacted the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801, *et seq.* (“FISA”) in response to concerns about surveillance abuses and illegalities perpetrated by the federal government.

11. FISA empowers the government to obtain *ex parte* judicial orders from the FISC Court authorizing domestic electronic surveillance by demonstrating, among other things, that probable cause exists to believe that the target is a foreign power or agent of a foreign power. 50 U.S.C. §§ 1804 (a) (3) and 1805 (a) (2). A foreign power is defined to include “a group engaged in international terrorism or activities in preparation therefor.” 50 U.S.C. § 1801.
12. In addition to arming the government with surveillance authority, 50 U.S.C. §§ 1801-1812, FISA was later amended to enable the government to obtain *ex parte* FISC orders authorizing physical searches, §§ 1821-1829, and pen registers and trap-and-trace devices, §§ 1841-1846.
13. In 1998, Congress added a “business records” provision to FISA. It empowered the FBI to apply for an *ex parte* order requiring specified entities, for instance, common carriers, to release business records by demonstrating that “there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.” 50 U.S.C. § 1862(b)(2)(B) (2000).
14. In the aftermath of the 9/11 terrorist attacks, Congress enacted the Patriot Act which, among other things, empowered the FBI under Section 215 to apply for a FISC order “requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.” 50 U.S.C. § 1861(a)(1).
15. Congress changed the standard for obtaining a Section 215 FISC order in 2006 by requiring an FBI application to include “a statement of facts 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 a United States person or to protect against international terrorism or clandestine intelligence activities.” 50 U.S.C. § 1861(b)(2)(A).

Mass Associational Tracking Program

16. Since May 2006, Defendants have conducted the Mass Associational Tracking Program under a series of FISC orders issued pursuant to Section 215. Upon information and belief, all major telecommunications companies operating in the United States provide NSA on an ongoing daily basis telephone metadata for all domestic and international telephone calls on their networks, including the calls of Plaintiffs and class members. Plaintiffs’ and class members’ metadata is collected, maintained, and periodically searched in a single database without any belief by Defendants at the time of collection or retention or searches that any of the information is connected with international terrorism or an international terrorist organization. Plaintiffs and class members hold subjective expectations of privacy over their collected, retained, and searched telephone metadata by Defendants, which expectations society views as reasonable. The MATP does not exempt the telephone metadata of anyone from its vast database.
17. Additionally, Defendants’ inconsistent public statements, along with now-public FISC orders, lead Plaintiffs and class members to be concerned that Defendants may have collected or may be collecting, storing, retaining, and searching location information from the telephone metadata.³ If Plaintiffs and class members learn that Defendants

³ For example, what is known as a “trunk identifier” is among the metadata included in the public orders of the FISC Court listing what is to be provided by a telephone company to the NSA. Trunk identifiers specify a physical

have or are collecting, storing, retaining, and searching location data relating to their telephone calls, Plaintiffs and class members reserve the right to move to amend their complaint accordingly. Additionally, upon information and belief, Defendants coordinate or have coordinated various metadata gathering programs to identify individuals and their personal information and relate such individuals to particular phone numbers, email addresses, etc.

18. Upon information and belief, there are over 300 million mobile phone subscribers in the United States, and approximately 100 million landline subscribers.
19. Telephone metadata collected by Defendants includes comprehensive communications routing information including, but not limited to, originating and terminating telephone number, International Mobile Subscriber Identity number, International Mobile Station Equipment Identity number, trunk identifier, telephone calling card numbers, and time and duration of call.
20. The metadata is stored by the NSA in repositories with secure networks, and access is restricted to authorized personnel with allegedly adequate and appropriate training.
21. The NSA is only to access the metadata to further an international terrorism investigation, and only by querying the entire database with a telephone number or identifier that is associated with an NSA-suspected foreign terrorist organization on a list approved by the FISC. The NSA refers to an identifier or phone number used to query the vast telephone metadata database as a “seed.” Such queries may only take

location where a call is connected between a single phone and a major element of the telecommunications network known as a “trunk.” Thus, having the trunk identifier that a caller connects to provides a rough location for that caller at the time the call is made and having the trunk identifier for the person being called also provides a rough location for the recipient of the call as well. Furthermore, if the NSA has received all of the trunk identifiers for each call (rather than merely the trunk identifiers connected to at the commencement of a phone call), then for calls made to or from phones that change location during the call, the NSA can roughly track such mobile phone user.

place after two NSA line personnel and one supervisor first decide that *they believe* there is “reasonable articulable suspicion” that the seed is associated with an international terrorist organization on the FISC approved list. There is no judicial oversight or appeal of such decision prior to NSA acting on the decision.⁴

22. The type and quantum of evidence needed to satisfy the “reasonable articulable suspicion” threshold to initiate a query by the NSA officials based on a seed is not publicly known. While the results do not identify the individuals or organizations associated with responsive telephone numbers, their identities (including the identities of Plaintiffs and class members) can be readily discovered outside the Mass Associated Tracking Program. When cross-checked against other public records, telephone metadata can reveal a person’s name, address, driver’s license, credit history, social security number, and other information.⁵
23. The results of a query also include second and third-tier contacts of the seed, referred to by the NSA as “hops.”
24. The first “hop” captures telephone metadata for phone numbers in direct contact with the seed.
25. The second “hop” reaches telephone metadata for telephone numbers in direct contact with the phone numbers captured in the first “hop.”
26. The third “hop” assembles telephone metadata for telephone numbers in direct contact with any second “hop” telephone number. The universe of telephone numbers that can

⁴ On December 15, 2005, then-Senator Barack Obama complained about the lack of judicial oversight on the floor of the Senate, stating: “If someone wants to know why their own government has decided to go on a fishing expedition through every personal record or private document, the library books that you’ve read, the phone calls that you made, the emails that you sent, this legislation gives people no rights to appeal the need for such a search in a court of law. No judge will hear your plea. No jury will hear your case. This is just plain wrong.” (emphasis added).

⁵ See *Klayman v. Obama*, 2013 U.S. Dist. LEXIS 176925, *94, n.58.

be within three hops of a seed over a five year period may easily run to the hundreds of thousands, absent reasonable restrictions.

27. Upon information and belief, since its commencement in May 2006, Defendants' Mass Associational Tracking Program has not stopped or been instrumental in stopping even one imminent international terrorist attack, or otherwise assisted Defendants in achieving any time-sensitive objective. The December 12, 2013, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies ("PRG")⁶ concluded that the Mass Associational Tracking Program "was not essential to preventing [terrorist] attacks and [the same information] could readily have been obtained in a timely manner using conventional Section 215 orders." PRG at 104.
28. Telephone metadata reveals a wealth of detail about Plaintiffs' and class members' familial, political, ideological, professional, religious, and other associations that are ordinarily unknown to government. *Klayman v. Obama*, 2013 U.S. Dist. LEXIS 176925, *94 (citing *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)). Such metadata and details taken by, and in the hands of, Defendants and government violate the reasonable expectations of privacy of Plaintiffs and class members.
29. A search occurs for purposes of the Fourth Amendment each time the NSA violates Plaintiffs' and class members' reasonable expectations of privacy. *ACLU v. Clapper*, 2013 U.S. Dist. LEXIS 180863, *63 (citing *Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring); *Jones* at 950 (2012); and *Bond v. United States*, 529

⁶ As of February 11, 2014, available at: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

U.S. 334, 337 (2000)). At a minimum, Defendants violate Plaintiffs' and class members' Fourth Amendment rights each time they gather, store or search Plaintiffs' and class members' telephone metadata.

30. That Plaintiffs and class members necessarily reveal certain information to telecommunications companies with which they contract for their telephone service – and which are provided to Defendants under the MATP – does not reflect a willingness or expectation that they are surrendering the privacy of the information, but simply reflects a necessary accommodation to modern life.⁷

⁷ See generally *Klayman v. Obama*, 2013 U.S. Dist. LEXIS 176925, *81-90; but see *Smith v. Maryland*, 442 U.S. 735 (1979).

The differences between the present case and *Smith* in both nature and scope are stark. A listing of such differences includes, but is not limited to, the following: (1) the fact that in *Smith*, the car owned by the target of the information-gathering had previously been spotted on the crime victim's street twice; whereas, in this case, there is no indication beforehand that any information gathered is related to anyone that has anything to do with any crime whatsoever. (2) The crime perpetrator in *Smith* was known to have used a phone to call the victim; whereas, in this case there is no known or suspected crime at the time of data collection. (3) The pen register in *Smith* was only operational for 13 days; whereas, in this case the government is essentially in a permanent cycle of ongoing collection. Thus, the sheer volume of data is exponentially different than in *Smith*. (4) There was no expectation the data gathered in *Smith* would be kept after the robbery case was over; whereas, in this case data is being gathered, stored, kept and searched for five years with no relation to any case whatsoever. (5) In *Smith*, the data gathered could have shown nothing about the movements of the caller; whereas the gathering of trunk identifying information under FISC orders can provide a general personal location aside from a fixed location. (6) The relationship between the government and the phone company in *Smith* was significantly different, i.e., limited in scope and cooperation; whereas, the daily and systematic exchange of all telephone metadata in this case spanning over seven-and-a-half years puts the telephone companies in a different posture than was the case in *Smith*. See *U.S. Dep't of Justice v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 764 (1989). (7) The ability of the government in *Smith* to address much more than one or a few phone numbers in any coordinated fashion simply did not exist; whereas, the technical capability of the government today to gather, store and search every, single phone number used to call or be called in the entire country was inconceivable to the Court in 1979, much less the authors of our Fourth Amendment. (8) In *Smith*, nothing but the date, time and phone numbers involved in a phone call were captured; whereas, with the MATP, phone numbers, rough location (via trunk identifier), whether or not a call was completed/connected, the date, time and duration of call, and a variety of details about the specific phones used on both ends of each phone call are obtained by the government. (9) In *Smith*, there were only landlines. There was no notion of a "mobile" phone, as there were no cellular phone systems in the U.S. until the 1980s; whereas, today the vast majority of American adults have a personal cell phone, and cellular telephone communication has reached a level of ubiquity such that our phone usage says much about us as individuals – something that was not even contemplated in 1979. Roughly the same proportion of adults had cell phones in 2013 (approx. 91%) [Joanna Brenner, *Pew Internet: Mobile* (Sept. 18, 2013), <http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx>] as households had phone lines in 1979 (approx. 91%) [U.S. Dep't of Commerce & U.S. Dep't of Hous. & Urban Dev., *Annual Housing Survey: 1979*, at 4 (1981) (Table A-1: Characteristics of the Housing Inventory: 1979 and 1970)].

31. Plaintiffs and class members reasonably expect both the ability to use telecommunications services and to maintain their privacy when they make phone calls, and society views such privacy expectations as reasonable.
32. The PRG observed (at 111-112): “In modern society, individuals, for practical reasons, have to use banks, credit cards, email, telephones, the Internet, medical services, and the like. Their decisions to reveal otherwise private information to such third parties does not reflect a lack of concern for the privacy of the information, but a necessary accommodation to the realities of modern life. What they want—and reasonably expect—is *both* the ability to use such services *and* the right to maintain their privacy when they do so.” (underlining added, italics in original).
33. Since the MATP was publicly disclosed, public opinion polls have shown widespread opposition to the dragnet collection, storage, retention, and search of telephone metadata collected on every domestic or international phone call made or received by citizens or permanent resident aliens in the United States.⁸ Such polling results are one form of evidence showing that society views as reasonable the subjective collective expectation of Plaintiffs and class members that telephone metadata related to their domestic and international communications will remain off limits to government collection, storage, retention, and search absent at least some reasonable, articulable suspicion or probable cause to believe that at the time of collection, storage, or search that such metadata is relevant to the investigation of a particular international terrorism investigation or other criminal enterprise.

⁸ See, e.g., *Associated Press, 9/11 Anniversary: Poll finds public doubts growing on federal surveillance, privacy*, Hous. Chron., Sept. 11, 2013, at A6 (“Some 56 percent oppose the NSA’s collection of telephone records for future investigations even though they do not include actual conversations.”).

34. Additional evidence that society views Plaintiffs' asserted privacy expectations in their telephone metadata as reasonable is shown by the ongoing efforts of an unusual number of states to oppose the NSA's MATP surveillance in their 2014 legislative sessions. These include Alaska, Arizona, California, Kansas, Maryland, Missouri, New Hampshire, Oklahoma, Tennessee, Vermont, and the State of Washington.⁹ Additionally, other states, including Virginia, are advancing legislation demonstrating their opposition to various forms of electronic surveillance without a warrant.¹⁰
35. The PRG underscored that abandoning the MATP would not disarm the United States in thwarting or punishing international terrorism, nor would it even stop the government from reasonable access to the same information: "[The government] would still be free under section 215 to obtain *specific* information relating to *specific* individuals on *specific* terrorist threats from banks, telephone companies, credit card companies, and the like—when it can demonstrate to the FISC that it has *reasonable grounds* to access such information." *Id* at 115.
36. The United States wields a formidable array of both traditional and relatively novel investigative powers, criminal prohibitions, and detention and killing authority to thwart or to punish international or domestic terrorism. On information and belief, the Mass Associational Tracking Program adds only speculatively – if at all – to the Executive Branch's muscular counterterrorism arsenal as elaborated herein. The PRG noted that the NSA for several years used a metadata program for Internet communications similar to the MATP under the authority of FISA's pen register and track-and-trace provisions rather than

⁹ As of February 11, 2014, information on the referenced legislative efforts in all of the cited states is available at: www.offnow.org/action/state.

¹⁰ On February 11, 2014, HB17, a bill requiring a warrant prior to the use of any tracking device, including but not limited to cellular phones with GPS or other tracking capability, passed the Virginia House of Delegates unanimously. <http://leg1.state.va.us/cgi-bin/legp504.exe?ses=141&typ=bil&val=hb17>.

Section 215. NSA suspended the program in 2009 for compliance reasons, re-started the program in 2010, and terminated the program in 2011. PRG at 97 n.91. According to Defendant Alexander, the Internet metadata program was terminated because it “was insufficiently productive to justify the cost.” *Id.* But according to Senator Wyden and Senator Mark Udall, the program was abandoned because Defendants were unable to demonstrate its effectiveness. Press Release, *Wyden, Udall Statement on the Disclosure of Bulk Email Records Collection Program* (July 2, 2013).¹¹

37. On March 12, 2013, during a Senate Intelligence Committee hearing, Defendant Clapper falsely stated in response to a question from Senator Ron Wyden (D-Ore.) that the NSA did not collect “any type of data at all on millions, or hundreds of millions, of Americans.” Hearing before Senate Intelligence Committee, March 12, 2013, transcript at 66.¹²

38. During a July 17, 2013, House Judiciary Committee hearing, Robert Litt, General Counsel of the Office of the Director of National Intelligence, answered the question of Chairman Robert Goodlatte (R-Va.), “Do you think a program of this magnitude, gathering information involving a large number of people involved with telephone companies and so on, could be indefinitely kept secret from the American people?” by responding, “Well, we tried.” Hearing before House Judiciary Committee, July 17, 2013, transcript at 14.¹³

¹¹ As of February 7, 2014, available at: <http://www.wyden.senate.gov/news/press-releases/wyden-udall-statement-on-the-disclosure-of-bulk-email-records-collection-program>.

¹² As of February 11, 2014, available at: <http://www.intelligence.senate.gov/pubcurrent.html>.

¹³ As of February 11, 2014, available at: <http://judiciary.house.gov/index.cfm/hearings?ID=37992064-B883-124D-1C4A-089A415C598E>.

search of the telephone metadata of class members violates the Fourth Amendment; and, whether declaratory and injunctive relief, including the purging of the telephone metadata concerning Plaintiffs and class members from Defendants' database, is appropriate.

43. **Typicality.** Plaintiffs' claims are typical of the claims of class members because they are based on the same legal theories and arise from the same conduct. Plaintiffs and class members were and are subscribers, users, and/or consumers of telephone service in the United States whose telephone metadata has been and continues to be collected, stored, retained, and searched by Defendants under the MATP as alleged herein.
44. **Adequacy.** Plaintiffs are adequate representatives of the class because their interests and the interests of class members they seek to represent do not conflict. The interests are virtually identical in seeking to prevent Defendants from collecting, storing, retaining, and searching telephone metadata related to Plaintiffs' and class members' domestic or international communications. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the class, and Plaintiffs have no interests antagonistic to the members of the class. Plaintiffs have retained counsel who is competent and experienced in the prosecution of class action litigation.
45. This suit may be maintained as a class action pursuant to Rule 23 (b)(2) of the Federal Rules of Civil Procedure because Defendants have acted on grounds that apply generally to the class, and final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole. Defendants' actions under the MATP do not differ with respect to the class members, and declaratory or injunctive relief is proper.

CLAIMS FOR RELIEF

46. Plaintiffs and class members re-allege each of the foregoing paragraphs.
47. Defendants' Mass Associational Tracking Program violates the Fourth Amendment rights of Plaintiffs and class members.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs and class members respectfully request that the Court:

1. Declare that the Mass Associational Tracking Program violates the Fourth Amendment to the Constitution;
2. Permanently enjoin Defendants from conducting or operating the MATP;
3. Order Defendants to purge from their possession, custody, and control all of the telephone metadata collected, stored, retained, and searched about Plaintiffs and class members pursuant to the MATP, regardless where held or by whom;
4. Certify the suit as a class action under Rule 23(b)(2) of the Federal Rules of Civil Procedure;
5. Issue an order establishing procedures enabling Plaintiffs' counsel to obtain required security clearances to adequately conduct discovery or otherwise litigate the case properly;
6. Award Plaintiffs' fees and costs pursuant to 28 U.S.C. 2412; and
7. Such other and further relief as the Court deems just and proper.