

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

LARRY KLAYMAN,
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006

and

CHARLES STRANGE,
Philadelphia, Pennsylvania

and

MARY ANN STRANGE,
Philadelphia, Pennsylvania

and

MICHAEL FERRARI,
Santa Clara, California

and

MATT GARRISON,
Long Beach, California

and

JEFFREY JAMES (“J.J.”) LITTLE,
Marina del Rey, California

by and on behalf of himself

and

J.J. LITTLE & ASSOCIATES, P.C.,
Marina del Rey, California

Plaintiffs,

v.

BARACK HUSSEIN OBAMA II, individually
and in his professional capacity,
1600 Pennsylvania Ave. NW
Washington, DC 20500

Civil Action No.: 13-cv-881-RJL

**THIRD AMENDED
COMPLAINT**

and

ERIC HIMPTON HOLDER, JR., individually
and in his professional capacity as U.S. Attorney General,
555 Fourth St. NW
Washington, DC 20530

and

KEITH B. ALEXANDER, individually
and in his professional capacity,
Director of the National Security Agency,
9800 Savage Rd.
Fort Meade, MD 20755

and

ROGER VINSON, individually and
in his professional capacity,
Judge, U.S. Foreign Intelligence Surveillance Court
950 Pennsylvania Ave. NW
Washington, DC 20530

and

JAMES CLAPPER, individually
and in his professional capacity,
Director of National Intelligence,
Washington, DC 20511

and

JOHN O. BRENNAN, individually
and in his professional capacity,
Director of the Central Intelligence Agency,
Central Intelligence Agency
Washington, DC 20505

and

JAMES COMEY, individually,
and in his professional capacity
Director Of The Federal Bureau Of Investigation
Federal Bureau Of Investigation
935 Pennsylvania Avenue, NW

Washington, DC 20535

and

NATIONAL SECURITY AGENCY,
9800 Savage Rd.
Fort Meade, MD 20755

and

THE U.S. DEPARTMENT OF JUSTICE,
950 Pennsylvania Ave. NW
Washington, DC 20530

and

FEDERAL BUREAU OF INVESTIGATION
935 Pennsylvania Avenue, NW
Washington, DC 20535

and

CENTRAL INTELLIGENCE AGENCY
Washington, DC 20505

Defendants.

THIRD AMENDED COMPLAINT

Plaintiffs, Larry Klayman, Charles and Mary Ann Strange, Michael Ferrari, Matthew Garrison, J.J. Little, and J.J. Little & Associates, P.C., (collectively “Plaintiffs”) bring this action on their own behalf and hereby sue Barack Hussein Obama II, Eric Holder, Keith B. Alexander, Roger Vinson, James Clapper, John O. Brennan, James Comey, the Federal Bureau of Investigation (“FBI”), the Central Intelligence Agency (“CIA”), the U.S. Department of Justice (“DOJ”), and the National Security Agency (“NSA”), (collectively “Defendants”), in their personal and official capacities, for violating Plaintiffs’ constitutional rights as a result of the below pled illegal unconstitutional acts. Plaintiffs allege as follows:

INTRODUCTION

1. This is an action for monetary, declaratory, equitable, and injunctive relief as a result of the U.S. Government's illegal and unconstitutional use of electronic surveillance programs in violation of the First, Fourth, and Fifth Amendments of the U.S. Constitution. In addition, this lawsuit challenges the Defendants' expansive acquisition of Plaintiffs' telephone metadata, Internet metadata and social media records under Section 215 of the Patriot Act, 50 U.S.C. § 1860 and the legality of a secret and illegal scheme to intercept and analyze vast quantities of communications from telephone, Internet and electronic service providers.
2. The NSA's classified surveillance program, referred to as "PRISM," is an internal government computer system, authorized by Section 702 of the Foreign Intelligence Surveillance Act ("FISA") (50 U.S.C. § 1881a), and is used to manage domestic and foreign intelligence collected from the Internet and other electronic service providers. Government officials have indicated this program has been in place for seven years and that it collects records of all communications companies including Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple, Verizon Business Network Services and Verizon Wireless ("Verizon"), AT&T, and Sprint.
3. Defendants have admitted that they are collecting metadata about every phone call made or received by residents and/or citizens of the United States, and these records provide intricate details, including the identity of the individual who was spoken to, the length of time of the conversation, and where the conversation took place. Moreover, it gives the Defendants a comprehensive record of an individual's associations, speech, and public

movements while revealing personal details about an individual's familial, political, professional, religious, and intimate associations.

4. For example, recently Defendants ordered access to Verizon's electronic copies of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. Such 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 identifier, telephone calling card numbers, and time and duration of call.
5. On June 5, 2013, The Guardian published an article, based on whistleblower Edward Snowden's revelations, all of which have never been controverted, entitled, "NSA collecting phone records of millions of Verizon customers daily. Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama." The Defendants, on the orders and authorization of the President, the Attorney General, the DOJ and the NSA, obtained a top secret court order ("Verizon Order") that directs Verizon to turn over the telephone records of over one hundred million Americans to the NSA on an ongoing daily basis. Based on knowledge and belief, this Verizon Order is the broadest surveillance order to ever have been issued; it requires no level of reasonable suspicion or probable cause and incredibly applies to all Verizon subscribers and users anywhere in the United States and overseas.

6. Prior to this disclosure and revelation, Plaintiffs had no notice and no reasonable opportunity to discover the existence of the surveillance program or the violation of the laws alleged herein.
7. Additionally, the NSA, CIA, and the FBI siphoned personal data from the main computer servers of major U.S. Internet firms, including Microsoft (Hotmail, etc.), Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple. The information the NSA receives in the surveillance and collection of stored communications include, e-mails, chat (video/voice), videos, photos, stored data, VoIP, file transfers, video conferencing, notification of target activity (i.e. logins, etc.), online social networking details, and other special requests.
8. It has become known that through a government program entitled "MUSCULAR," the FBI, CIA, and NSA have been intercepting information of the entirety of American citizenry from Internet companies such as Google and Yahoo! as it travels over fiber optic cables from one data center to another.
9. Such broad and intrusive collections and surveillance tactics, without regard to any showing of probable cause, much less a reasonable suspicion of communications with terrorists or the commission of another crime, directly violate the U.S. Constitution and also federal laws, including, but not limited to, the outrageous breach of privacy, freedom of speech, freedom of association and the due process rights of American citizens. Plaintiffs are suing for damages, declaratory, equitable, and injunctive relief to stop this illegal conduct and hold Defendants, individually and collectively, responsible for their unconstitutional surveillance, which has violated the law and damaged the fundamental freedoms and rights of American citizens.

10. While the Government Defendants represented that the bulk collection of Internet metadata pursuant to Section 215 was discontinued in 2011, this representation was false. The Government Defendants simply played a shell-game where they shifted the unconstitutional acts from Section 215 over to their continuing PRISM program under Section 702. This was revealed by Defendant James Clapper's admissions to Senator Ron Wyden. *See* Exhibits 3 and 4, incorporated herein by reference.

THE PARTIES

11. Plaintiff Larry Klayman is an individual and an international attorney who is a subscriber and user of Verizon Wireless, Vonage, Apple, Microsoft, YouTube, Yahoo, Google, Facebook, Twitter, AT&T, and Skype at all material times. Klayman routinely communicates with members of the public as well as journalists and associates by telephonic communications and electronic messages through Facebook, Google, Apple, and Skype. Klayman's communications, particularly as an attorney, are sensitive and often privileged. Plaintiff Klayman resided in the District of Columbia ("D.C.") for over twenty years and continues to conduct business in Washington, D.C. as the Chairman and General Counsel of Freedom Watch and otherwise. Plaintiff Larry Klayman is a public advocate and has filed lawsuits against President Obama and has been highly critical of the Obama administration as a whole. Defendants have accessed the records pertaining to Plaintiff Klayman.
12. Plaintiff Klayman frequents and routinely telephones and e-mails individuals and high-ranking government officials in Israel, a high-conflict area where the threat of terrorism is always present. U.S. and Israeli intelligence agencies are constantly monitoring the telecommunications in Israel in order to prevent any future attacks by terrorists.

13. While in Israel, most recently in 2009, 2010, and 2012, Klayman met with the Press Secretary for Prime Minister Benjamin Netanyahu, Mr. Mark Regev, as well as Daniel B. Shapiro, who is now the U.S. Ambassador to the United States to the State of Israel. Plaintiff Klayman also communicates with Mr. Regev internationally via telephone and e-mail. In 2012 Plaintiff Klayman was in Jerusalem and Tel Aviv during the war with Hamas and experienced rocket attacks while he was in Tel Aviv.
14. Plaintiff Klayman also met with Ron Nachman who was mayor of the city of Ariel, Israel until his death in 2013. Plaintiff Klayman remained in telephone and e-mail communication with Mr. Nachman and his aides after his visit to Israel. Importantly, Ariel is located in Judea, which Palestinians and other Arabs falsely call "Occupied Territory." Judea is a breeding ground for terrorists.
15. Plaintiff Klayman has also telephoned and e-mailed Danny Danon, a member of Israel's Knesset (legislative body), who is currently serving as the Deputy Minister of Defense in the Cabinet of Prime Minister Benjamin Netanyahu.
16. In addition, Plaintiff has been in telephone and e-mail contact with Aaron Klein in Israel, an investigative reporter who hosts a radio show on WABC in New York, which originates in Israel. In fact, Klayman was recently interviewed by Aaron Klein regarding the NSA, during which time the radio show experienced what the host called "a tech meltdown." Specifically, software used by the radio station "dropped" Plaintiff Klayman from the phone line and listeners who had called in to ask Klayman questions were cut out in mid-sentence. It is clear that the NSA was attempting to harass him, Aaron Klein, and anyone connected to this show, many of whom had been critical of the Defendants, including President Obama.

17. Plaintiff Klayman also telephoned and e-mailed individuals within Spain in preparation for his visit to Spain in July of 2012 where he met with prominent human rights lawyers to discuss bringing an action against the Islamic Republic of Iran and its officials for violations of human rights. Plaintiff continued communication with those he met in Spain following his visit. Prior to this, Plaintiff Klayman telephoned and e-mailed individuals in India in preparation for his trip to India in 2007, where he served process on the Prime Minister of India. Similarly, in May of 2012, Plaintiff Klayman traveled to the headquarters of the Organization of the Petroleum Exporting Countries ("OPEC") located in Vienna, Austria in order to personally serve it with process and has made calls to Austria in this regard. Among OPEC's members is the Islamic Republic of Iran, and other Islamic states, which further, harbor and/or have close ties to terrorism. In fact, the oil revenues of OPEC help fund terrorism and terrorists bent on destroying the United States, its ally Israel, and other western and European interests. Plaintiff Klayman also routinely sends and receives e-mails and telephone communications to and from Italy, France, Great Britain, Morocco, Germany, Belgium and other European Union nations which have very large Muslim populations and where terrorist cells are located and thus where terrorist attacks have been perpetrated resulting in numerous deaths and maimed persons.
18. In light of Plaintiff Klayman's foreign contacts and communications, including frequent telephone calls and e-mail correspondence domestically and internationally, Defendants would have inevitably been monitoring Plaintiff Klayman in the ordinary course of their surveillance. In fact, given Plaintiff Klayman's contacts in the regions he has traveled to,

Plaintiff Klayman was undoubtedly targeted by Defendants and his domestic and foreign communications gathered and surveilled.

19. Plaintiffs Charles Strange and Mary Ann Strange are individuals and the parents of Michael Strange, a Navy cryptologist assigned to SEAL Team VI who was killed when the helicopter he was in was attacked and shot down by terrorist Taliban jihadists in Afghanistan on August 6, 2011. Plaintiffs Charles and Mary Ann Strange are consumers, subscribers, and users of Verizon Wireless, Google/Gmail, Yahoo, Facebook, AOL, and YouTube. Plaintiff Charles Strange is a subscriber of Verizon Wireless. Plaintiff Mary Ann Strange is also a subscriber of Verizon Wireless. On information and belief, Defendants have accessed Plaintiff Stranges' records particularly since these Plaintiffs have been vocal about their criticism of President Obama as commander-in-chief, his administration, and the U.S. military regarding the circumstances surrounding the shoot down of their son's helicopter in Afghanistan, which resulted in the death of his son and other Navy SEAL Team VI members and special operation forces. Plaintiffs Charles Strange and Mary Ann Strange have substantial connections with Washington, D.C., as they hold press conferences in Washington, D.C. and lobby in Washington, D.C. as advocates for Michael Strange and to obtain justice for him, as well as to change the policies and orders of President Obama and the U.S. military's acts and practices, which contributed to Michael Strange's death. Plaintiffs Charles and Mary Ann Strange also make telephone calls and send and receive e-mails to and from foreign countries and have received threatening e-mails and texts from overseas, in particular Afghanistan.
20. Plaintiff Ferrari is an individual who is a subscriber, consumer, and user of Sprint, Google/Gmail, Yahoo!, and Apple. As a prominent private investigator, Ferrari regularly

communicates, both telephonically and electronically, with associates and other members of the public, regarding various matters including work-related discussions. Additionally, Ferrari's e-mails contain private details, discussions, and communications. Similarly, Ferrari's Apple products contain confidential documents and information. Plaintiff Ferrari also makes and receives telephone calls and sends and receives e-mails to and from foreign countries.

21. Plaintiff Garrison is an individual who is a consumer and user of Facebook, Google, YouTube, and Microsoft products. Plaintiff Garrison is required to use his computer, which contains Microsoft programming, for personal matters as well as work related matters, as a prominent private investigator. Plaintiff stores various documents and records on his computer, which are private records. Plaintiff Garrison also makes and receives telephone calls and sends and receives e-mails to and from foreign countries.
22. Plaintiff J.J. Little is an individual and a criminal defense lawyer and a member of the California and Ohio Bars. He has litigated and continues to litigate against the Government on behalf of his clients. He is therefore in the line of fire of Government surveillance by the Government Defendants. This implicates breaches of attorney-client privilege and work product. At all material times, Plaintiff Little, for himself and by and through his law firm, J.J. Little & Associates, has been and continues to be a subscriber of Verizon Business Network Services for his firm J.J. Little & Associates, P.C. At all material times, both J.J. Little and J.J. Little & Associates are subscribers of Verizon Business Network Services and Verizon Wireless. Plaintiffs Little and J.J. Little & Associates, P.C. also use and subscribe to the Internet and social media, as set forth herein.

23. Each and every Plaintiff uses and subscribes to the enumerated telephonic, Internet and social media communications providers and uses these services both domestically and internationally.
24. Defendant Barack Hussein Obama ("Obama") is the President of the United States and currently resides in Washington, D.C.
25. Defendant Eric Holder ("Holder") is the Attorney General of the United States and conducts his duties as the Attorney General in Washington, D.C.
26. Defendant Keith B. Alexander ("Alexander") is the Director of the National Security Agency. He is also the commander of the U.S. Cyber Command, where he is responsible for planning, coordinating, and conducting operations of computer networks. He is also at the command for U.S. National Security Information system protection responsibilities. He conducts his duties for the National Security Agency in Washington, D.C.
27. Defendant Roger Vinson ("Vinson") is a judge to the U.S. Foreign Intelligence Surveillance Court.
28. Defendant James Clapper ("Clapper") is currently the Director of National Security and conducts his duties as the Director of National Security in Washington, D.C.
29. Defendant John O. Brennan ("Brennan") is currently the Director of the Central Intelligence Agency and conducts his duties in Washington, D.C.
30. Defendant James Comey ("Comey") is currently the Director of the Federal Bureau of Investigation and conducts his duties in Washington, D.C.
31. Defendant National Security Agency ("NSA") is an intelligence agency of the U.S. Department of Defense and conducts its duties in Washington, D.C.

32. Defendant U.S. Department of Justice ("DOJ") is responsible for the enforcement of the law and administration of justice, and its headquarters is located in Washington, D.C., where it conducts most of its activities and business.
33. Defendant Central Intelligence Agency ("CIA") is responsible for providing national security intelligence to senior U.S. policymakers and conducts its duties in Washington, D.C.
34. Defendant Federal Bureau of Investigation ("FBI") is a governmental agency belonging to the U.S. Department of Justice that services as an internal intelligence agency and conducts its duties in Washington, D.C.
35. All of these Defendants, each and every one of them, jointly and severally, acted in concert to violate the constitutional privacy rights, free speech, freedom of association, due process, and other legal rights of Plaintiffs.

JURISDICTION AND VENUE

36. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1331 (Federal Question Jurisdiction).
37. Jurisdiction and venue are proper pursuant to 28 U.S.C. § 1331, which 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." At issue here is the unconstitutional violation of Plaintiffs' rights under the First, Fourth, and Fifth Amendments to the U.S. Constitution.
38. Supplemental jurisdiction is also proper under 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.”

39. Plaintiffs are informed, believe and thereon allege that, based on the places of business of the Defendants and/or on the national reach of Defendants, a substantial part of the events giving rise to the claims herein alleged occurred in this district and that Defendants and/or agents of Defendants may be found in this district.

STANDING

40. Plaintiffs bring this action because they have been directly affected, victimized, and severely damaged by the unlawful conduct complained herein. Their injuries are proximately related to the egregious, illegal, unconstitutional and indeed criminal acts of Defendants Obama, Holder, Alexander, Comey, Brennan, Vinson, Clapper, FBI, CIA, DOJ and NSA, each and every one of them, jointly and severely, acting in their personal and official capacities.

STATEMENT OF FACTS

41. Defendants, through the NSA and CIA, and with the participation of certain telecommunications and Internet companies, have conducted surveillance and intelligence-gathering programs that collect certain data about the telephone and Internet activity of American citizens within the United States. In fact, the NSA began a classified surveillance program, known as “PRISM,” used to intercept telephonic and Internet communications of persons inside the United States and overseas.
42. As recently discovered, on June 5, 2013, The Guardian reported the first of several “leaks” of classified material from Edward Snowden, a former NSA contract employee who has revealed – and continues to reveal—multiple U.S. Government intelligence

collection and surveillance programs. Specifically, The Guardian published an article entitled, "NSA collecting phone records of millions of Verizon customers daily.

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama." Pursuant to this top-secret order, issued by Judge Roger Vinson, the Government, on the orders and authorization of the President, the Attorney General, the DOJ, and the NSA, obtained a highly classified order directing Verizon to turn over the telephone records of over one hundred million Americans to the NSA on an ongoing daily basis.

43. Specifically, Defendant Vinson ordered access to electronic copies of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. 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 identifier, telephone calling card numbers, and time and duration of call. Defendant Vinson's Order further required Verizon to turn over originating and terminating telephone numbers as well as the location, time, and duration of the calls. In essence, the Order gives the NSA blanket access to the records of over one hundred million of Verizon customers' domestic and foreign phone calls made between April 25, 2013, when the Order was signed, and July 19, 2013, when the Order is supposed to, on its face, expire.

44. Based on knowledge and belief, this Order issued by Defendant Vinson is the broadest surveillance order to ever have been issued; it requires no level of reasonable suspicion or probable cause and incredibly applies to all Verizon subscribers and users anywhere in the United States and overseas.
45. Defendant Vinson's Order shows for the first time that, under Defendant Obama's administration, the communication records of over one hundred million 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.
46. Since June 5, 2013, Defendants have been widely condemned by American citizens regarding their failure to uphold the U.S. Constitution and intentionally violating the fundamental rights of Plaintiffs and over one hundred million of other Americans, particularly as new information comes to light regarding the Defendants' countless surveillance programs and intrusive overreaching tactics. As just one example, Senator Rand Paul called the surveillance of Verizon phone records "an astounding assault on the Constitution," calling for a class action lawsuit.
47. Such schemes by the Defendants have subjected untold numbers of innocent people to the constant surveillance of government agents. As Jameel Jaffer, the ACLU's deputy legal director, stated, "It 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." Recently the Court agreed, calling the Defendants' programs "almost Orwellian" and stating that the Court "cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and

retention of personal data on virtually every single citizen for purposes of querying it and analyzing it without judicial approval.”

48. To date, Defendants have not issued substantive and meaningful explanations to the American people describing what has occurred. Rather, on information and belief, the NSA, under the authorization of President Obama, continues to engage in a systematic program of warrantless eavesdropping upon phone, e-mail, Internet, and social media communications of hundreds of millions of individuals, including American citizens and permanent legal residents, both within and outside of the United States. The NSA surveillance program collects not only the identities of people's communications with the targets of surveillance, but also the contents of those communications.
49. Such intrusive and illegal surveillance has directly impacted each and every Plaintiff. The revelation that the Defendants have been carrying on widespread warrantless interception of electronic communications has impaired Plaintiffs’ abilities to communicate via telephone, e-mail, social media and otherwise on the Internet, out of fear that their confidential, private, and often privileged communications are being and will be overheard by the NSA’s surveillance program.
50. The risk and knowledge that Plaintiffs’ telephonic, Internet and social media conversations may be overheard, undoubtedly chills speech, in violation of Plaintiffs’ First Amendment rights.
51. It was disclosed on August 12, 2015 by Charlie Savage of The New York Times that Verizon Wireless, as this Court had already ruled in its Order of December 16, 2013, at all material times was conducting and continuing to conduct unconstitutional and illegal dragnet “almost-Orwellian” surveillance on Plaintiffs and millions of other American

citizens. *See* Exhibit 1, which is a Government document evidencing this, incorporated herein by reference, and *see* Exhibit 2, the New York Times article.

52. The Government Defendants withheld this document, dated August 2, 2010 – for *five* years– and caused the U.S. Court of Appeals for the District of Columbia Circuit to issue a decision based on an incomplete and false record. The Government Defendants and their counsel had a duty to supplement the record and failed to do so in contravention of the rules of professional responsibility and in violation of 18 U.S.C. § 1001, as the omission was intentional, among other violations of law.
53. In addition, the Government Defendants misled this Court and the U.S. Court of Appeals for the District of Columbia Circuit by playing a shell-game whereby they falsely represented that they ceased accessing Internet metadata and other data through Section 215 in 2011, when it is now apparent and has been revealed based on Clapper’s admissions to Senator Ron Wyden that they simply moved, at all material times, this unconstitutional metadata collection violation of the Fourth, First and Fifth Amendment rights over to their continuing PRISM program under Section 702. *See* Exhibits 3 and 4, incorporated herein by reference.
54. The Government Defendants, through the use of the continuing PRISM and MUSCULAR programs, illegally and unconstitutionally surveilled each of the Plaintiffs’ telephone, Internet and social media communications.

FIRST CLAIM FOR RELIEF

Fifth Amendment Violation

**Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey,
Brennan, FBI, CIA, DOJ and NSA
(Bivens v. VI Unknown Named Agents of Federal Bureau of Narcotics)**

55. Plaintiffs repeat and reallege all of the previous allegations in paragraphs 1 through 54 of this Third Amended Complaint with the same force and affect, as if fully set forth herein again at length.
56. Plaintiffs enjoy a liberty interest in their personal security and in being free from the Defendants' use of unnecessary and excessive force or intrusion against his person.
57. Plaintiffs enjoy a liberty of not being deprived of life without due process of law, as guaranteed by the Fifth Amendment to the U.S. Constitution.
58. Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA violated Plaintiffs' constitutional rights when they authorized broad and intrusive collections of records of individuals through the PRISM and MUSCULAR surveillance programs, thereby giving Defendants authority to obtain telephone and Internet data for a specified amount of time.
59. By reason of the wrongful conduct of the Defendants, each and every one of them, jointly and severally, Plaintiffs suffered and continue to suffer from severe emotional distress and physical harm, pecuniary and economic damage, loss of services, and loss of society accordingly.
60. These violations are compensable under *Bivens v. VI Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971). As a direct and proximate result of the intentional and willful actions of Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, Plaintiffs demand judgment be entered against Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, each and every one of them, jointly and severally, including an award of compensatory and actual damages, punitive damages, equitable

relief, reasonable attorneys fees, pre-judgment interest, post-interest and costs, and an award in an amount in excess of \$20 billion U.S. dollars, and such other relief as the Court may deem just and proper. Plaintiffs declaratory and injunctive and other equitable relief against all of Defendants as set forth below.

SECOND CLAIM FOR RELIEF

First Amendment Violation

**Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey,
Brennan, FBI, CIA, DOJ and NSA
(Bivens v. VI Unknown Named Agents of Federal Bureau of Narcotics)**

61. Plaintiffs repeat and reallege all of the previous allegations in paragraphs 1 through 60 of this Third Amended Complaint with the same force and affect, as if fully set forth herein again at length.
62. Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, acting in their official capacity and personally, abridged and violated Plaintiffs' First Amendment right of freedom of speech and association by significantly minimizing and chilling Plaintiffs' freedom of expression and association.
63. Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA's acts chill, if not "kill," speech by instilling in Plaintiffs and over a hundred million of Americans the fear that their personal and business conversations with other U.S. citizens and foreigners are in effect surveilled, tapped, and illegally surveyed.
64. In addition, Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, acting in their official capacity and personally, violated Plaintiffs' right of freedom of association by making them and others weary and fearful of contacting other persons and entities via cell phones, the Internet, or through social media out of fear of the misuse of government power and retaliation against these persons

and entities who challenge the gross misuse of government power which amounts to an almost Orwellian police state.

65. By reason of the wrongful conduct of these Defendants, Plaintiffs suffered and continue to suffer from severe emotional distress and physical harm, pecuniary and economic damage, loss of services, and loss of society accordingly.
66. These violations are compensable under *Bivens v. VI Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971).
67. As a direct and proximate result of the intentional and willful actions of Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, Plaintiffs demand that judgment be entered against Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, each and every one of them, jointly and severally, including an award of compensatory and actual damages, punitive damages, equitable relief, reasonable attorneys fees, pre-judgment interest, post-interest and costs, and an award in an amount in excess of \$20 billion U.S. dollars and such other relief as the Court may deem just and proper.

THIRD CLAIM FOR RELIEF

Fourth Amendment Violation

**Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey,
Brennan, FBI, CIA, DOJ and NSA
(*Bivens v. VI Unknown Named Agents of Federal Bureau of Narcotics*)**

68. Plaintiffs repeat and reallege all of the previous allegations in paragraphs 1 through 67 of this Complaint with the same force and affect, as if fully set forth herein again at length.
69. The Fourth Amendment provides in pertinent part that people have a right 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 search must be described with particularity.

70. Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, acting in their official capacities and personally, violated the Fourth Amendment to the U.S. Constitution when they unreasonably searched and seized and continue to search Plaintiffs' phone records, e-mails, Internet, social media and electronic communications without reasonable suspicion or probable cause.
71. Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, acting in their official capacity and personally, violated the Fourth Amendment to the U.S. Constitution by not describing with particularity the place to be searched or the person or things to be seized.
72. In fact, the blanket and vastly overbroad surveillance program by the NSA, acting on behalf of the federal government and therefore Defendant Obama, as he is the chief executive of the federal government, as well as the other Defendants, does not state with any particularity who and what may be searched.
73. The collection and production of the phone, e-mail, Internet, and social media records allows Defendants including the FBI, CIA, and NSA to easily and indiscriminately build a comprehensive picture and profile of any individual contacted, how and when he or she was contacted, and possibly from where, retrospectively and into the future.
74. By reason of the wrongful conduct of Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, Plaintiffs suffered and continue to suffer from severe emotional distress and physical harm, pecuniary and economic damage, loss of services, and loss of society accordingly.

75. These violations are compensable under *Bivens v. VI Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971). As a direct and proximate result of the intentional and willful actions of Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA, Plaintiffs demand judgment be entered against Defendants Obama, Holder, Alexander, Vinson, Clapper, Comey, Brennan, FBI, CIA, DOJ and NSA each and every one of them, jointly and severally, including an award of compensatory and actual damages, punitive damages, equitable relief, reasonable attorneys fees, pre-judgment interest, post-interest and costs, and an award in an amount in excess of \$20 billion U.S. dollars and such other relief as the Court may deem just and proper.

PRAYER FOR RELIEF

76. Plaintiffs demand that judgment be entered against Defendants, each and every one of them, jointly and severally, for compensatory and actual damages because of Defendants' illegal actions causing this demonstrable injury to Plaintiffs, punitive damages because of Defendants' callous, reckless indifference and malicious acts, and attorneys fees and costs in an amount in excess of \$20 billion U.S. dollars and such other relief the Court may deem just and proper.
77. Plaintiffs demand declaratory, equitable and injunctive relief for their injuries in the following ways: (1) a cease and desist order to prohibit this type of illegal and criminal activity against Plaintiffs and other U.S. citizens from occurring now and in the future; (2) that all Plaintiffs' phone, e-mail, Internet, and social media records and communication records, whether telephonic, Internet, social media or electronic, be returned to the provider and expunged from federal government records; and (3) a full

disclosure and a complete accounting of what each Defendant as a whole has done and allowed the DOJ, CIA, FBI, and NSA to do; and (4) that this Court retain jurisdiction to implement an effective judicial monitoring mechanism to insure that the Defendants do not egregiously continue, after they are enjoined, to violate the constitutional rights of the Plaintiffs and all Americans in the future, particularly since the Foreign Surveillance Intelligence Court, through judges such as Defendant Vinson, has colluded or acquiesced with Defendants in their unlawful conduct. Defendants cannot, given their documented pattern of lying under oath, deceit and unlawful unconstitutional conduct, be left on their own, without court supervision, to obey the law.

JURY DEMAND

Plaintiffs respectfully demand a jury trial on all issues so triable.

Dated: September 8, 2015

Respectfully submitted,

/s/ Larry Klayman

Larry Klayman, Esq.

D.C. Bar No. 334581

2020 Pennsylvania Ave. NW, Suite 345

Washington, DC 20006

Tel: (310) 595-0800

Email: leklayman@gmail.com

Attorney for Plaintiffs

Exhibit 1



U.S. Department of Justice

National Security Division SURVEILLANCE

2010 AUG -2 PM 4:32

TOP SECRET//COMINT//NOFORN

Washington, D.C. 20530

The Honorable John D. Bates
United States Foreign Intelligence Surveillance Court
U.S. Courthouse
333 Constitution Avenue, N.W.
Washington, D.C. 20001

Re: Compliance Incident Involving In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from AT&T, the Operating Subsidiaries of Verizon Communications Inc., and Celco Partnership d/b/a Verizon Wireless, and Sprint Relating to al Qaeda and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with al Qaeda and Associated Terrorist Organizations and the Government of Iran and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with the Government of Iran and Associated Terrorist Organizations, Docket Number BR 10-10. (TS)

Dear Judge Bates:

Pursuant to Rule 10(c) of the Foreign Intelligence Surveillance Court (FISC) Rules of Procedure, effective February 17, 2006, this letter further advises the Court of a compliance incident regarding docket number BR 10-10. A preliminary notice regarding the incident was filed with the Court on July 26, 2010. (S)

On February 26, 2010, in docket number BR 10-10, Judge Reggie B. Walton approved an application for tangible things. Judge Walton renewed that authority on May 14, 2010, in docket number BR 10-17, expiring on August 6, 2010. The Court's Primary Order in docket number BR 10-10 states: "The BR metadata may be accessed for the purposes of ensuring data integrity and developing and testing any technological measures designed to enable the NSA to comply with the Court's orders." Docket Number BR 10-10, Primary Order at 5. "Persons who query the BR metadata pursuant to this paragraph may only share the results of any such query with other specially-cleared NSA technical personnel," with limited exceptions, including when "a data integrity analyst [DIA] conduct[s] the query using a RAS-approved telephone identifier at the request of an analyst authorized to query the BR metadata" *Id.* at 5-6. (TS//SI//NF)

On July 16, 2010, the National Security Agency (NSA) advised the Department of Justice's National Security Division of the compliance incident described below:

TOP SECRET//COMINT//NOFORN

Classified by: David S. Kris, Assistant
Attorney General, NSD, DOJ

Reason: 1.4(c)

Declassify on: 2 August 2035

TOP SECRET//COMINT//NOFORN

- On March 9, 2010, a DIA queried the BR metadata in response to a Federal Bureau of Investigation (FBI) request for certain information relating to a United States telephone identifier referenced in a previously issued NSA report. Specifically, the FBI inquired whether the BR metadata contained information indicating that the identifier was roaming during in the [REDACTED] to [REDACTED] time frame. (TS//SI//NF)
- The reasonable, articulable suspicion (RAS) approval for the identifier expired on [REDACTED], [REDACTED], [REDACTED] before the query. (It had been RAS-approved on [REDACTED], [REDACTED].) Still, the identifier was listed on the Station Table – historically, NSA's list of identifiers that have undergone RAS determinations – as RAS-approved until [REDACTED], [REDACTED] at which time its status was changed to "not approved." (TS//SI//NF)
- The DIA used the identifier to conduct a single query of the BR metadata in the Transaction Database. Although the preliminary notice of this incident reported that the query was time-bounded to the period of [REDACTED] through [REDACTED], the query was not time-bounded. Rather, the DIA focused his review of the query results to the time period referenced in the FBI's request for information. (TS//SI//NF)
- Based on the query results, the DIA determined that no roaming data was available for the identifier, and NSA provided that information to the FBI. NSA did not issue a report based on this query. (TS//SI//NF)

This incident was discovered by the staff of NSA's Inspector General through their review of controls used to comply with the Court's Orders in this matter. NSA confirms that it conducted no queries using the identifier after the DIA's query described above. (TS//SI//NF)

At the time of this incident, NSA managed the RAS-approval status of identifiers on the Station Table through a periodic, manual review of those identifiers. NSA assesses that this compliance incident resulted from delays in the manual review process. NSA further assesses that a technical modification likely will prevent this sort of compliance incident from occurring in the future. In June 2010, NSA implemented a new program to manage and track requests to approve the use of identifiers that meet the RAS standard. This new program, among other things, automatically changes an identifier's status to "not approved" if it has not been re-approved for RAS within the time frame specified by the Court's orders. (TS//SI//NF)

[REDACTED], Global Capabilities Manager, Counterterrorism, reviewed a draft of this letter and confirmed its accuracy. (U)

Sincerely,

[REDACTED]
Section Chief, Oversight
National Security Division
U.S. Department of Justice

cc: The Honorable Reggie B. Walton

TOP SECRET//COMINT//NOFORN

Exhibit 2

U.S.

N.S.A. Used Phone Records Program to Seek Iran Operatives

By CHARLIE SAVAGE AUG. 12, 2015

WASHINGTON — The National Security Agency has used its bulk domestic phone records program to search for operatives from the government of Iran and “associated terrorist organizations” — not just Al Qaeda and its allies — according to a document obtained by The New York Times.

The document also shows that a February 2010 order from the Foreign Intelligence Surveillance Court for the program listed AT&T and Sprint as involved in it. A leaked 2013 court order for the program was addressed only to a Verizon subsidiary.

The inclusion of Iran and allied terrorist groups — presumably the Shiite group Hezbollah — and the confirmation of the names of other participating companies add new details to public understanding of the once-secret program. The Bush administration created the program to try to find hidden terrorist cells on domestic soil after the attacks of Sept. 11, 2001, and government officials have justified it by using Al Qaeda as an example.

The disclosure of the new details comes at a time of debates over a proposed agreement to drop sanctions against Iran in exchange for curbs on its nuclear program, and about N.S.A. surveillance and the role of American communications companies.

In June, Congress enacted a law that will ban the systematic collection of domestic phone records after November, and create a replacement program for analyzing links between callers in search of associates of terrorism suspects without the government's keeping the bulk data.

The document disclosing new information about the program is an August 2010 letter from the Justice Department to Judge John Bates, then the presiding judge of the intelligence court. It was included in about 350 pages of N.S.A. inspector general reports about the program the government provided to The Times late on Tuesday in response to a Freedom of Information Act suit.

The letter, which alerted Judge Bates to an incident in which a court-imposed rule for the program had been violated, contained information the government usually redacts when declassifying such documents: the full name of the intelligence court order in place for the program at the time, which included the listing of Iran and the names of the companies. The release of the uncensored version of the letter was apparently a mistake.

The N.S.A. did not respond to a request for comment.

President George W. Bush originally directed the N.S.A. to begin systematically collecting Americans' calling records in bulk based on a unilateral assertion of executive power. In 2006, the Justice Department persuaded the intelligence court to bless the program. It began issuing orders to phone companies to turn over their customers' calling records.

Its orders were based on a secret interpretation of a provision of the U.S.A. Patriot Act, known as Section 215, which permits the F.B.I. to obtain business records deemed "relevant" to a national security investigation.

The theory, accepted by the intelligence court but rejected in a recent appeals court ruling, is that everyone's records are relevant to investigations hunting for terrorists because analyzing indirect links between callers can, in

theory, reveal hidden relationships and sleeper cells.

After praising the program as crucial to preventing terrorist attacks, intelligence agency officials now say that it has never thwarted one. But the program's proponents argue that it is still a useful investigative tool.

The program became public in June 2013 after Edward J. Snowden, a former N.S.A. contractor, disclosed a trove of the agency's classified documents. The first of those published was the 2013 intelligence court order to a Verizon subsidiary requiring it to turn over all its customers' calling records.

Although the Obama administration declassified the existence of the bulk phone records program, it has declined to confirm which other phone companies participated in it and which groups it could be used to search for.

The letter does not make clear how often the N.S.A. has used the program to search for Iran or Iranian-linked terrorist organizations. It also says nothing further about the companies listed in the case name.

There has been wide speculation that AT&T, which maintains a large database of calling records, was a participant in the program. And last year, when the government declassified documents about an aborted challenge to the program by a phone company in late 2009, it redacted the firm's name, but officials said it was Sprint.

The Justice Department letter confirms that both of those companies have been participants.

But the document also contained a surprise. In addition to listing subsidiaries of Verizon Communications, the document lists Verizon Wireless, which was then a partnership with the British firm Vodafone.

The inclusion of Verizon Wireless was striking. In June 2013, The Wall Street Journal reported that Verizon Wireless and T-Mobile had not been part

of the classified program because of their foreign ownership stakes. In 2014, The Journal, The Washington Post and The Times each reported, citing intelligence officials, that for technical reasons, the program consisted mostly of landline phone records.

However, it is not clear whether the inclusion of Verizon Wireless in the name of the court order means it was turning over customer records after all.

Ed McFadden, a Verizon spokesman, said he was not permitted to say whether that was the case. But he said that as a general matter, it has been the government's practice to use broad language covering all of Verizon's entities in headings of such court orders because it has a complex corporate structure, regardless of whether any specific part was required to provide information under that order.

Most of the inspector general reports, unlike the letter, contained redactions. They showed that the inspector general in 2006, shortly after the pre-existing program came under the intelligence court's rules, called for greater procedural safeguards to make sure that the new rules were followed.

There were no reports included in the documents from 2007 to 2009, when it came to light internally that the N.S.A. had been accessing the call records in a way that systematically violated the court's rules. In late 2009, the intelligence court stopped letting the N.S.A. access the bulk data for operational purposes while it built a new system and tested it. There were many reports from 2010 and 2011, when the court ordered the inspector general to conduct a series of audits.

One document also reveals a new nugget that fills in a timeline about surveillance: a key date for a companion N.S.A. program that collected records about Americans' emails and other Internet communications in bulk. The N.S.A. ended that program in 2011 and declassified its existence after the Snowden disclosures.

In 2009, the N.S.A. realized that there were problems with the Internet records program as well and turned it off. It then later obtained Judge Bates's permission to turn it back on and expand it.

When the government declassified his ruling permitting the program to resume, the date was redacted. The report says it happened in July 2010.

A version of this article appears in print on August 13, 2015, on page A14 of the New York edition with the headline: N.S.A. Used Phone Data to Seek Iran Operatives.

© 2015 The New York Times Company

Exhibit 3

MAR 28 2014

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

During the January 29, 2014, Worldwide Threat hearing, you cited declassified court documents from 2011 indicating that NSA sought and obtained the authority to query information collected under Section 702 of the Foreign Intelligence and Surveillance Act (FISA), using U.S. person identifiers, and asked whether any such queries had been conducted for the communications of specific Americans.

As reflected in the August 2013 Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702, which we declassified and released on August 21, 2013, there have been queries, using U.S. person identifiers, of communications lawfully acquired to obtain foreign intelligence by targeting non U.S. persons reasonably believed to be located outside the U.S. pursuant to Section 702 of FISA. These queries were performed pursuant to minimization procedures approved by the FISA Court as consistent with the statute and the Fourth Amendment. As you know, when Congress reauthorized Section 702, the proposal to restrict such queries was specifically raised and ultimately not adopted.

For further assistance, please do not hesitate to contact Deirdre M. Walsh in the Office of Legislative Affairs, at (703) 275-2474.

Sincerely,



James R. Clapper

Exhibit 4

NSA Admits to Wrongdoing—What Now?

Andrew Napolitano | Apr. 10, 2014 7:00 am



Pete Souza/White House

Last week, Director of National Intelligence James R. Clapper sent a brief letter to Sen. Ron Wyden (D-Ore.), a member of the Senate Intelligence Committee, in which he admitted that agents of the National Security Agency (NSA) have been reading innocent Americans' emails and text messages and listening to digital recordings of their telephone conversations that have been stored in NSA computers, without warrants obtained pursuant to the Constitution. That the NSA is doing this is not newsworthy—Edward

Snowden has told the world of this during the past 10 months. What is newsworthy is that the NSA has *admitted* this, and those admissions have far-reaching consequences.

Since the Snowden revelations first came to light last June, the NSA has steadfastly denied them. Clapper has denied them. The recently retired head of the NSA, Gen. Keith Alexander, has denied them. Even President Obama has stated repeatedly words to the effect that "no one is reading your emails or listening to your phone calls."

The official NSA line on this has been that the Foreign Intelligence Surveillance Act (FISA) court has issued general warrants for huge amounts of metadata only, but not content. Metadata consists of identifying markers on emails, text messages, and telephone calls. These markers usually identify the computer from which an email or text was sent or received, and the time and date of the transmission, as well as the location of each computer. Telephone metadata is similar. It consists of the telephone numbers used by the callers, the time, date, and duration of the call, and the location of each telephone used in the call.

American telecommunications and Internet service providers have given this information to the NSA pursuant to warrants issued by secret FISA court judges. These warrants are profoundly unconstitutional, as they constitute general warrants. General warrants are not

obtained by presenting probable cause of crime to judges and identifying the person from whom data is to be seized, as the Constitution requires. Rather, general warrants authorize a government agent to obtain whatever he wants from whomever he wants it.

These general warrants came about through a circuitous route of presidential, congressional, and judicial infidelity to the Constitution during the past 35 years. The standard that the government must meet to obtain a warrant from a FISA court judge repeatedly has been lessened from the constitutional requirement of probable cause of crime, to probable cause of being a foreign agent, to probable cause of being a foreign person, to probable cause of talking to a foreign person. From this last category, it was a short jump for NSA lawyers to persuade FISA court judges that they should sign general warrants for all communications of everyone in America because the NSA was not accessing the content of these communications; it was merely storing metadata and then using algorithms to determine who was talking to whom.

This was all done in secret—so secret that the president would lie about it; so secret that Congress, which supposedly authorized it, was unaware of it; and so secret that the FISA court judges themselves do not have access to their own court records (only the NSA does).

It was to further this public facade that Clapper lied to the Senate Intelligence Committee last year when he replied to a question from Sen. Wyden about whether the NSA was collecting massive amounts of data on hundreds of millions of Americans by saying, "No" and then adding, "Not wittingly." The stated caveat in the NSA facade was a claim that if its agents wanted to review the content of any data the NSA was storing, they identified that data and sought a warrant for it.

This second round of warrants is as unconstitutional as the first round because these warrants, too, are based on NSA whims, not probable cause of crime. Yet, it is this second round of warrants that Clapper's letter revealed did not always exist.

Snowden, in an act of great personal sacrifice and historic moral courage, directly refuted Clapper by telling reporters that the NSA possessed not just metadata but also content—meaning the actual emails, text messages, and recordings of telephone calls. He later revealed that the NSA also has the content of the telephone bills, bank statements, utility bills, and credit card bills of everyone in America.

In his letter to Wyden last week, Clapper not only implicitly acknowledged that Snowden was correct all along, but also that he, Clapper, lied to and materially misled the Senate Intelligence Committee, and that the NSA is in fact reading emails and listening to phone calls without obtaining the second warrant it has been claiming it obtains.

One wonders whether Obama was duped by Clapper when he denied all this, or whether he just lied to the American people as he has done in the past.

One also wonders how the government could do all this with a straight face. This is the same government that unsuccessfully prosecuted former New York Yankees pitcher Roger Clemens twice for lying to a congressional committee about the contents of his urine. Shouldn't we expect that Clapper be prosecuted for lying to a congressional committee about the most massive government plot in U.S. history to violate the Fourth Amendment? Don't hold your breath; the president will protect his man.

Yet, Congress could address this independent of a president who declines to prosecute his fellow liars. Congress could impeach Clapper, and the president would be powerless to prevent that. If Congress does that, it would be a great step forward for the rule of law and fidelity to the Constitution. If Congress does nothing, we can safely conclude that it is complicit in these constitutional violations.

If Congress will not impeach an officer of the government when it itself is the victim of his crimes because it fears the political consequences, does it still believe in the Constitution?