Ilann M. Maazel (*pro hac vice*)
Matthew D. Brinckerhoff (*pro hac vice*)
Adam R. Pulver (SBN # 268370)
EMERY CELLI BRINCKERHOFF & ABADY LLP
75 Rockefeller Plaza, 20th Floor
New York, New York 10019
Telephone: (212) 763-5000
Facsimile: (212) 763-5001
Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION This Document Relates to: VIRGINIA SHUBERT, NOHA ARAFA, SARAH DRANOFF and HILARY BOTEIN, individually and on behalf of all others similarly situated, Plaintiffs, -against - BARACK OBAMA, KEITH B. . ALEXANDER, ERIC HOLDER, MICHAEL HAYDEN, ALBERTO GONZALES, JOHN ASHCROFT, UNITED STATES OF AMERICA, and JOHN/JANE DOES #1-100 (07-693)	Case No. 3:06-md-1791-VRW **SECOND AMENDED CLASS ACTION COMPLAINT/ DEMAND FOR JURY TRIAL**

Plaintiffs Virginia Shubert, Noha Arafa, Sarah Dranoff, and Hilary Botein, by their attorneys Emery Celli Brinckerhoff & Abady LLP, for their Second Amended Complaint, allege as follows:

PRELIMINARY STATEMENT

1. This class action challenges a secret government spying program pursuant to which, on information and belief, virtually every telephone, Internet and email communication sent from or received within the United States since shortly after September 11, 2001 has been (and continues to be) searched, seized, intercepted, and subjected to surveillance without a warrant, court order or any other lawful authorization in violation of the Foreign Intelligence Surveillance Act of 1979, 50 U.S.C. § 1810.

2. Without the approval of Congress, without the approval of any court, and without notice to the American people, President George W. Bush authorized a secret program to spy upon millions of innocent Americans, including the named plaintiffs. As one former NSA employee admitted, "The National Security Agency had access to *all* Americans' communications: faxes, phone calls, and their computer communications . . . It didn't matter whether you were in Kansas, you know, in the middle of the country and you never made foreign communications at all. They monitored all communications."[1] This program (the "Spying Program") – intercepting, searching, seizing, and subjecting to surveillance the content of personal phone conversations, email, and Internet searches of millions of unsuspecting, innocent Americans – is illegal. It violates the plain terms of federal statutes that make such conduct a crime.[2] It violates the most basic principles of separation of powers. It violates the Constitution.

3. The government's spy agency, the National Security Agency ("NSA"), spied upon Americans at home. It spied upon Americans at work. And it is spying today, and will continue to spy on millions of innocent, unsuspecting Americans, unless stopped by a federal court.

4. The existence and operation of this secret spying program has been acknowledged by numerous executive officials, including former President Bush in December

---

[1] http://www.youtube.com/watch?v=osFprWnCjPA at 2:15 (statement by NSA operative Russell Tice).

[2] *E.g.* The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* ("FISA"); the Wiretap Act 18 U.S.C. § 2510 *et seq.*; the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* ("SCA").

2005, former Attorney General Alberto Gonzales and former Director of National Intelligence Michael Hayden, as well as high-level officials in the NSA.

5. As part of the Spying Program, defendants have not only eavesdropped on specific communications by American citizens, they have also intercepted and continue to intercept *en masse* the communications of millions of ordinary Americans – estimated at between 15 and 20 *trillion* communications over the past eleven years.

6. Defendants have achieved this dragnet in part by attaching sophisticated communications surveillance devices to the key facilities of numerous telecommunications companies, including AT&T and Verizon (used by the named plaintiffs), that transmit and receive Americans' Internet and telephone communications.

7. Using these surveillance devices, defendants have acquired and continue to acquire the content of phone calls, emails, instant messages, text messages, web communications and other communications, both international and domestic, of millions of Americans who use the phone system or the Internet, including Plaintiffs and class members.

8. Having unlawfully acquired and intercepted millions of communications from United States persons, the NSA searches for keywords, phrases, or names it deems suspicious, in order to select which communications are subjected to yet further analysis by staff of the NSA, as part of a vast data-mining operation.

9. The American people deserve better. The American people should not be subjected to a illegal, covert, dragnet spying operation by their own government. This class action is brought on behalf of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant, court order, or other lawful authorization since September 12, 2001.[3] It primarily seeks liquidated damages under the Federal Intelligence Surveillance Act 50 U.S.C. § 1810 *et. seq.* ("FISA"), which authorizes civil actions for violations of FISA.

---

[3] "United States persons" and "electronic surveillance" are both defined terms set forth in FISA. 50 U.S.C. § 1801.

PARTIES

10. Plaintiff Virginia Shubert is an American citizen who resides and works in Brooklyn, New York. Ms. Shubert regularly makes phone calls and sends email both within the United States, and outside the United States. Ms. Shubert, for example, frequently calls and sends emails to the United Kingdom, France and Italy and has made similar communications as a part of her work. Since September 12, 2001, Ms. Shubert has been and continues to be a customer of AT&T, which participated and participates in the Spying Program. Pursuant to the illegal Spying Program, Ms. Shubert's phone calls and emails have repeatedly been surveilled and intercepted by the NSA without a warrant or other judicial authorization. On information and belief, Ms. Shubert's illegally intercepted communications are currently in the custody, control, and possession of the NSA.

11. Plaintiff Noha Arafa is an American citizen who resides and works in Brooklyn, New York. She regularly makes phone calls and sends email both within the United States, and outside the United States. Ms. Arafa, for example, frequently calls and sends emails to family and friends in Egypt from her home, and has made telephone calls abroad as a part of her work. Since September 12, 2001, Ms. Dranoff has been and continues to be a customer of a customer of AT&T, which participated and participates in the Spying Program. Pursuant to the illegal Spying Program, Ms. Arafa's phone calls and emails have repeatedly been surveilled and intercepted by the NSA without a warrant or other judicial authorization. On information and belief, Ms. Arafa's illegally intercepted communications are currently in the custody, control, and possession of the NSA.

12. Plaintiff Sarah Dranoff is an American citizen who resides and works in Brooklyn, New York. Ms. Dranoff regularly makes phone calls and sends email both within the United States, and outside the United States. Ms. Dranoff for example, calls the Netherlands and sends emails to the Netherlands and Norway from her home. Since September 12, 2001, Ms. Dranoff has been a customer of Verizon and of AT&T, which, on information and belief, participated and participates in the Spying Program. Pursuant to the illegal Spying Program, Ms. Dranoff's phone calls and emails have repeatedly been surveilled and intercepted by the NSA

without a warrant or other judicial authorization. On information and belief, Ms. Dranoff's illegally intercepted communications are currently in the custody, control, and possession of the NSA.

13. Plaintiff Hilary Botein is an American citizen who resides and works in Brooklyn, New York. Ms. Botein makes phone calls and sends email both within the United States, and outside the United States. Since September 12, 2001, Ms. Botein has been a customer of Verizon which, on information and belief, participated and participates in the Spying Program. Pursuant to the illegal Spying Program, Ms. Botein's phone calls and emails have repeatedly been surveilled and intercepted by the NSA without a warrant or other judicial authorization. On information and belief, Ms. Botein's illegally intercepted communications are currently in the custody, control, and possession of the NSA.

14. Defendant Barack H. Obama is the President of the United States, and sued solely in his official capacity. Mr. Obama's predecessor, George W. Bush, authorized the illegal Spying Program, and Mr. Obama has continued and continues to authorize the illegal Spying Program.

15. Defendant Lieutenant General Keith B. Alexander is the Director of the NSA, and is sued in both his personal and official capacities. Since 2005, Defendant Alexander has had ultimate authority for supervising and implementing all operations and functions of the NSA, including the illegal Spying Program.

16. Defendant Eric Holder is the Attorney General of the United States, and is sued solely in his official capacity. On information and belief, Mr. Holder approved and authorized the Spying Program. Mr. Holder's predecessor, Defendant Gonzales approved and authorized the Spying Program and has consistently defended the program before Congress and in other public fora.

17. Defendant Lieutenant General Michael V. Hayden is the former Director of the NSA, and is sued solely in his personal capacity. While Director, defendant Hayden had ultimate authority for supervising and implementing all operations and functions of the NSA,

including the illegal Spying Program.. Defendant Hayden also apparently approved the illegal initiation of the Spying Program.

18. Defendant Alberto Gonzales is the former Attorney General of the United States. Defendant Gonzales approved and authorized the Spying Program and has consistently defended the program before Congress and in other public fora.

19. Defendant John Ashcroft is the former Attorney General of the United States. Although, according to some published reports, defendant Ashcroft had reservations concerning the Spying Program, Mr. Ashcroft ultimately approved and authorized the Spying Program.

20. Each of the individual defendants works or worked for the government of the United States of America, which has conducted and continues to conduct the illegal Spying Program.

21. At all times relevant hereto, defendants John and Jane Does #1-100 (the "Doe defendants"), whose actual names plaintiff has been unable to ascertain notwithstanding reasonable efforts to do so, but who are sued herein by the fictitious designation "John Doe" and "Jane Doe," were agents and employees of the NSA, Department of Homeland Security, Department of Justice, the White House, or other government agencies, acting in the capacity of agents, servants, and employees of the United States government, and within the scope of their employment as such, who conducted, authorized, and/or participated in the Spying Program.

JURISDICTION AND VENUE

22. This action arises under the Fourth Amendment to the United States Constitution, the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, the Wiretap Act 18 U.S.C. § 2510 *et seq.*; and the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*

23. The jurisdiction of this Court is predicated upon 28 U.S.C. §§ 1331, 1343(a)(4).

24. Venue is proper in this transferee district pursuant to an Order of the Judicial Panel on Multi-District Litigation, pursuant to 28 U.S.C. § 1407, and is proper in the transferor district (Eastern District of New York), pursuant to 28 U.S.C. § 1391(e).

JURY DEMAND

25. Plaintiffs demand trial by jury in this action.

CLASS ACTION ALLEGATIONS

26. The plaintiff class seeks (i) a judgment declaring that the Spying Program violates FISA, the Wiretap Act, the SCA, and the Fourth Amendment; (ii) an order enjoining defendants from continuing the Spying Program or otherwise subjecting United States persons to electronic surveillance by the NSA without a search warrant or court order; (iii) an order requiring defendants to delete and destroy, permanently and irrevocably, every communication and record of every communication intercepted by the NSA pursuant to the Spying Program in the custody, control, or possession of the United States or any of its agents or employees; and (iv) liquidated damages as set forth in 50 U.S.C. § 1810, and 18 U.S.C. §§ 2520, 2707 to redress the extraordinary invasion of privacy caused by the Spying Program.

27. Plaintiffs sue on behalf of themselves and all other similarly situated individuals, and seek to represent a class comprised of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant, court order, or other lawful authorization since September 12, 2001.

28. The members of the class are so numerous as to render joinder impracticable.

29. The questions of law and fact common to the class include that the class members were all subject to electronic surveillance without a search warrant, court order, or any lawful authorization pursuant to the Spying Program; all have the common right under FISA, the Wiretap Act, and the SCA to be free from electronic surveillance absent a search warrant or court order, the common right under FISA, the Wiretap Act, and the SCA to liquidated damages for violations of those rights, and the common right under the Fourth Amendment to be free from electronic surveillance absent a search warrant or court order. Defendants' electronic surveillance without a search warrant, court order, or any lawful authorization violated those rights.

30. The named plaintiffs are adequate representatives of the class. The violations of law alleged by the named plaintiffs stem from the same course of conduct by defendants – failure to seek a search warrant, court order, or any other lawful authorization before conducting electronic surveillance – that violated and continue to violate the rights of members of the class; the legal theory under which the named plaintiffs seek relief is the same or similar to that on which the class will rely. In addition, the harms suffered by the named plaintiffs are typical of the harms suffered by the class members, especially given the common calculation of liquidated damages.

31. The named plaintiffs have the requisite personal interest in the outcome of this action and will fairly and adequately protect the interests of the class. The named plaintiffs are represented by Emery Celli Brinckerhoff & Abady LLP ("ECBA"). Counsel has the resources, expertise and experience to prosecute this action. Counsel for the plaintiffs knows of no conflicts among members of the class or between ECBA and members of the class.

32. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because: (i) the prosecution of millions of separate actions would be inefficient and wasteful of legal resources; (ii) the members of the class are scattered throughout the United States and are not likely to be able to vindicate and enforce their statutory and constitutional rights unless this action is maintained as a class action; (iii) the issues raised can be more fairly and efficiently resolved in the context of a single class action than piecemeal in many separate actions; (iv) the resolution of litigation in a single forum will avoid the danger and resultant confusion of possible inconsistent determinations; (v) the prosecution of separate actions would create the risk of inconsistent or varying adjudications with respect to individuals pursuing claims against defendants which would establish incompatible standards of conduct for defendants; and (vi) questions of law and/or fact common to members of the class predominate over any question that affects individual members.

FACTUAL ALLEGATIONS

Classwide Allegations

Legal Framework

33. The Fourth Amendment provides that "[t]he 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."

34. Congress has enacted two statutes that together supply "the *exclusive means* by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f) (emphasis added). The first is the Electronic Communications Privacy Act ("ECPA"), which includes the Wiretap Act, 18 U.S.C. § 2510 *et seq*., and the Stored Communications Act, 18 U.S.C. § 2701 *et seq*., and the second is the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* ("FISA").

The ECPA

35. Congress first enacted the predecessor to the ECPA (commonly referred to as Title III) in response to the U.S. Supreme Court's recognition, in *Katz v. United States*, 389 U.S. 347 (1967), that individuals have a constitutionally protected privacy interest in the content of their telephone calls. Through Title III and then the ECPA, Congress created a statutory framework to govern the surveillance of wire and oral communications in law enforcement investigations.

36. The ECPA authorizes the government to intercept wire, oral, or electronic communications in investigations of certain enumerated criminal offenses, *see* 18 U.S.C. § 2516, with prior judicial approval, *see id.* § 2518.

37. In order to obtain a court order authorizing the interception of a wire, oral, or electronic communication, the government must demonstrate that "there is probable cause for belief that an individual is committing, has committed, or is about to commit" one of the enumerated criminal offenses. *Id.* § 2518(3)(a).

38. It must also demonstrate, among other things, that "there is probable cause for belief that particular communications concerning [the enumerated] offense will be obtained through [the] interception," *id.* § 2518(3)(b), and that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," *id.* § 2518(3)(c).

39. The ECPA specifies civil and criminal penalties for surveillance that is not authorized. *See id.* §§ 2511, 2520, 2701, 2707.

Foreign Intelligence Surveillance Act

40. The government has one and only one other legal avenue to engage in electronic surveillance: the Foreign Intelligence Surveillance Act.

41. In 1978, Congress enacted FISA to govern the use of electronic surveillance against foreign powers and their agents inside the United States. The statute created the Foreign Intelligence Surveillance Court, a court composed of seven (now eleven) federal district court judges, and empowered this court to grant or deny government applications for electronic surveillance orders in foreign intelligence investigations. *See* 50 U.S.C. § 1803(a). Congress enacted FISA after the U.S. Supreme Court held, in *United States v. United States District Court for the Eastern District of Michigan,* 407 U.S. 297 (1972), that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. FISA was a response to that decision and to the Report of the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, S.Rep. No. 94-755, 94th Cong., 2d Sess. (1976) ("Church Committee Report"), which found that the executive had engaged in warrantless wiretapping of numerous United States citizens – including journalists, activists, and Congressmen – who posed no threat to the nation's security and who were not suspected of any criminal offense. The Church Committee Report warned that "[u]nless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature."

42. When Congress enacted FISA, it provided that the procedures set out therein "shall be the *exclusive means* by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f) (emphasis added).

43. FISA provides that no one may engage in electronic surveillance "except as authorized by statute," *id.* § 1809(a)(1).

44. FISA specifies civil and criminal penalties for electronic surveillance undertaken without statutory authority, *see id.* §§ 1809 & 1810.

45. The Senate Judiciary Committee explained that "[t]he basis for this legislation is the understanding – concurred in by the Attorney General – that even if the President has an 'inherent' Constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance." S. Rep. 95-604(I), reprinted at 1978 U.S.C.C.A.N. at 3917. The Committee further explained that the legislation was meant to "spell out that the executive cannot engage in electronic surveillance within the United States without a prior Judicial warrant." *Id.* at 3906.

46. FISA defines "electronic surveillance" to include:

a. "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes";

b. "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire

communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States . . .";

c. "the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States"; and

d. "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f).

47. FISA defines "contents" to include "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 50 U.S.C. § 1801(n).

48. FISA defines "United States person" to include United States citizens and lawful permanent residents. *Id.* § 1801(d).

49. In order to obtain an order from the FISA Court authorizing electronic surveillance, the government must demonstrate, among other things, probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and that

"each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(3).

50. While FISA generally prohibits surveillance without prior judicial authorization, it includes a provision that allows for warrantless surveillance in "emergency situation[s]." Where an emergency situation exists and "the factual basis for issuance of an order under this subchapter to approve such surveillance exists," the statute permits the Attorney General to authorize warrantless surveillance "if a judge having jurisdiction under section 1803 of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this subchapter is made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance." *Id.* § 1805(f).

51. FISA also permits electronic surveillance without a court order for fifteen days after a formal declaration of war. *Id.* § 1811 ("Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.").

52. FISA requires the Attorney General to report to the House and Senate Intelligence Committees twice a year regarding "all electronic surveillance" authorized under FISA. *Id.* § 1808(a). Statistics released annually by the Justice Department indicate that, between 1978 and 2004, the government submitted almost 19,000 surveillance applications to the FISA Court. The FISC denied four of these applications; granted approximately 180 applications with modifications; and granted the remainder without modifications.

The Creation of the Spying Program

53. Until December 2005, even the existence of the Spying Program was unknown to Congress and to the American people.

54. To the contrary, in a speech on June 9, 2005, President Bush stated: "*Law enforcement officers need a federal judge's permission to wiretap a foreign terrorist's phone, a federal judge's permission to track his calls, or a federal judge's permission to search his property.*

Officers must meet strict standards to use any of these tools. And these standards are fully consistent with the Constitution of the U.S." (Emphasis supplied.)[4]

55. Although it is true that federal law requires law enforcement officers to get permission from a federal judge to wiretap, track, or search, President Bush secretly authorized a Spying Program that did none of those things.

56. As revealed in *The New York Times* in December 2005, and as subsequently revealed by, *inter alia*, published press reports, whistleblowers, insiders within the United States government, top government officials, and (after initial equivocation) President Bush himself, in the fall of 2001 the NSA launched a secret electronic surveillance program to intercept, search and seize, without prior judicial authorization, the telephone and Internet communications of people inside the United States. This program, as Rep. Silvestre Reyes, then-Chairman of the House Permanent Select Committee On Intelligence (who has been briefed on the Program), explained at a September 2007 hearing, "involved not only targets overseas, but also American citizens whose phone calls were listened to and e-mail read without a warrant."

57. On or around October 4, 2001, President Bush issued an order authorizing the NSA to conduct surveillance of telephone and Internet communications of persons within the United States, without court-approved warrants or other judicial authorization. The Spying Program began on or around October 6, 2001. While President Bush ultimately signed the Program Order initiating the Program, Vice President Cheney and the legal counsel to the Office of the Vice President, David Addington, "guided the program's expansion and development." According to one former DOJ Official, Addington was the "chief legal architect" of the Program, and he and Cheney "had abhorred FISA's intrusion on presidential power ever since its enactment in 1978. After 9/11 they and other top officials in the administration dealt with FISA the way they dealt with other laws they didn't like: They blew through them in secret based on flimsy legal opinions that they guarded closely so no one could question the legal basis for the operations."

---

[4] *See* http://georgewbush-whitehouse.archives.gov/news/releases/2005/06/20050609-2.html.

58. President Bush reauthorized the Spying Program more than 30 times between October 2001 and December 2006, approximately every 45 days, as confirmed by responses by the Office of the Vice President to a Congressional subpoena.

59. The Program reflects a goal of the NSA presented to the incoming Bush administration in December 2000. A transition document for the new administration stated "The volumes and routing of data make finding and processing nuggets of intelligence information more difficult. To perform both its offensive and defensive mission, NSA must 'live on the network.'" Moreover, the NSA asserted that its "mission will demand a powerful, permanent presence on a global telecommunications network that will host the 'protected' communications of Americans as well as the targeted communications of adversaries."

60. Addington and then-White House Counsel Alberto Gonzales assigned John Yoo, then a Deputy Assistant Attorney General in the Office of Legal Counsel, to prepare legal opinions in support of the Program. The Department of Justice prepared memoranda dated October 4 and November 2, 2001; January 9, May 17, and October 11, 2002; February 25, 2003; March 15, May 6, and July 16, 2004; and February 4, 2005. Years later, after he left government service in 2003, Yoo explained why FISA was not sufficient for the Program's dragnet interception:

> [U]nder existing laws like FISA, you have to have the name of somebody, have to already suspect that someone's a terrorist before you can get a warrant. You have to have a name to put in the warrant to tap their phone calls, and so it doesn't allow you as a government to use judgment based on probability to say: "Well, 1 percent probability of the calls from or maybe 50 percent of the calls are coming out of this one city in Afghanistan, and there's a high probability that some of those calls are terrorist communications. But we don't know the names of the people making those calls." You want to get at those phone calls, those e-mails, but under FISA you can't do that.

61. The government has candidly admitted that FISA "requires a court order before engaging in this kind of surveillance . . . unless otherwise authorized by statute or by Congress." The Program admittedly operates "in lieu of" court orders or other judicial authorization, and neither the President nor Attorney General authorizes the specific interceptions. As General (Ret.) Michael V. Hayden, the former Principal Deputy Director for National Intelligence, put it, the Program "is a more . . . 'aggressive' program than would be traditionally available under FISA," in part because "[t]he trigger is quicker and a bit softer than it is for a FISA warrant." The only review process is authorization by an NSA "shift supervisor" for direct review of particular individuals' communication.

The Mechanics of the Spying Program

62. As part of the Spying Program, the NSA uses satellite dishes controlled both by the NSA and those controlled by telecommunications companies to intercept, search and seize, and subject to electronic surveillance communications that are transmitted via satellite. Many of these satellite dishes are located within the United States.

63. According to the Senate Select Committee on Intelligence, shortly after September 11, 2011, the Executive branch sent letters requesting or directing U.S. electronic communication service providers to provide access to communications in order to assist the NSA with intelligence activities that had been authorized by the President. In a Report, the Committee confirmed: "The letters were provided to electronic communication service providers at regular intervals. All of the letters stated that the activities had been authorized by the President. All of the letters also stated that the activities had been determined to be lawful by the Attorney General, except for one letter that covered a period of less than sixty days. That letter, which like all the others stated that the activities had been authorized by the President, stated that the activities had been determined to be lawful by the Counsel to the President."

64. The "assistance" sought involved an important aspect of the Spying Program challenged here. The NSA uses electronic communication companies, including AT&T and Verizon (used by the named plaintiffs), to intercept, search and seize, and subject to electronic surveillance communications, including voice calls and e-mails, that pass through switches

controlled by these companies. These switches are the hubs through which voice calls and data transmissions are routed every second.

65. These switches, which are located inside the United States, serve as primary gateways for communications going into, through, and out of the United States. The switches connect to transoceanic fiber-optic cables that transmit communications to other countries.

66. In January 2006, a former AT&T employee named Mark Klein provided detailed eyewitness testimony and documentary evidence showing how telecommunications companies in general, and AT&T in particular, are acquiring communications for the government. Klein had worked as an AT&T technician for 22 years, most recently at AT&T's San Francisco facility on Folsom Street.

67. The NSA has worked with telecommunications and Internet providers in the United States to install "splitters" on fiber-optic cables carrying domestic and international communications. According to William Binney, the former chief and co-founder of the NSA's Signals Intelligence Automation Research Center, and a former senior NSA crypto-mathematician, there are between 10 and 20 such splitters installed throughout the country—"not just San Francisco; they have them in the middle of the country and also on the East Coast."[5] The installation of these splitters allows two identical copies of all communications to be made, with one copy traveling its intended course, and the other being routed to the NSA. These communications are routed *en masse* to the NSA without any concern for the subject matter or content of the communications.

68. Former AT&T employee Klein has provided documents showing how these splitters operate, and divert communications to the NSA, at one AT&T facility. To divert the communications, AT&T connected the fiber-optic cables entering its WorldNet Internet room to a "splitter cabinet." The splitter cabinet splits the light signals from the WorldNet Internet service in two, making two identical copies of the material carried on the light signal. The splitter cabinet

[5] James Bamford, "The NSA is Building the Country's Biggest Spy Center (Watch What You Say)," Wired *Threat Level* Blog (Mar. 15, 2012), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/; also available as James Bamford, "Inside the Matrix," *Wired*, April 2012, at 78.

directs one portion of the light signal through fiber optic cables into a secret room built on AT&T premises, but controlled by the NSA while allowing the other portion to travel its normal course to its intended destination. The split cables carry domestic and international communications of AT&T customers, as well as communications from users of other non-AT&T networks that pass through that facility. The position or location of the fiber split make clear that it was not designed to capture only international traffic, and necessarily captures purely domestic communications, as a fiber splitter is not a selective device. According to Klein, AT&T intercepts every single one of the communications passing through the WorldNet Internet room and directs them all to the NSA. Klein and others have reported similar splitters throughout the United States. Klein's report has been confirmed by James Russell, AT&T's Managing Director-Asset Protection.

69. According to former NSA official Binney, at the outset of this program, the NSA recorded 320 million calls a day – a number that has since increased.[6]

70. After the communications are acquired by the NSA, they are subjected to an initial computer-controlled analysis to "listen" to the content of the communications, search for targeted addresses, locations, countries, phone numbers, keywords, phrases, and watch-listed names, and analyze patterns, referred to by former Secretary of Homeland Security Michael Chertoff as "data-mining." This analysis intrudes into content, and the computers "listen" to more Americans than humans do. The Program uses extremely powerful computerized search programs—originally intended to scan foreign communications—to scrutinize large volumes of American communications. According to a recent article based on interviews with former NSA officials, "Any communication that arouses suspicion, especially to or from the million or so people on agency watch lists, are automatically copied or recorded,"[7] and subjected to human review. Once an individual has been "flagged," all calls and communications to or from that individual are automatically routed to the NSA's recorders.

71. Government officials have acknowledged that "most telephone calls in the United States" are subjected to such searches, regardless of whether there was any suspicion of the

---

[6] *Id.*
[7] *Id.*

sender or recipient. As one official explained, "you have to have all the calls or most of them. But you wouldn't be interested in the vast majority of them."

72. One way communications are searched is by keywords. If the keywords included "jihad," "Iraq," "Bush is a criminal," or whatever words or phrases the United States government deems of interest, then, pursuant to the Spying Program, the Americans who use such terms may be targeted by the NSA for even further interception, search and seizure, and electronic surveillance.

73. As reported in *The Wall Street Journal*, the data-sifting effort can also begin by using a phone number or web address as a lead. "In partnership with the FBI, the systems then can track all domestic and foreign transactions of people associated with that item -- and then the people who associated with them, and so on, casting a gradually wider net. An intelligence official described more of a rapid-response effect: If a person suspected of terrorist connections is believed to be in a U.S. city -- for instance, Detroit, a community with a high concentration of Muslim Americans -- the government's spy systems may be directed to collect and analyze all electronic communications into and out of the city."

74. NSA employees have also confirmed that they have personally listened in on hundreds of citizens' phone calls that have no connection to national security, including calls between Americans and their family members abroad and calls regarding international aid organizations.

75. NSA employees have also admitting listing to calls simply for their own entertainment – specifically calls that are in some way tantalizing and salacious – and sharing the calls of these private, personal conversations with office mates.

76. As one former NSA employee, Adrienne Kinne, has explained, NSA interceptors often found themselves listening to "incredibly intimate, personal conversations." She noted, "It's almost like going through and finding somebody's diary."

77. Prior to human review, all the acquired communications, including those to, from and/or between Americans, are stored in a vast government database for potential future use. As Director of National Intelligence ("DNI") J. Michael McConnell later explained, immediately

after acquisition "[t]here is no human that is aware of it. So you wouldn't know that until you went into the database." The NSA is currently building a large facility known as the "Utah Data Center," where it is believed these and other communications will be stored in the future. This information is apparently kept indefinitely, even if the subject of the surveillance is an ordinary American. *Trillions* of domestic communications with no intelligence value are acquired and stored in the database.

78. On the occasions where the government follows procedures established to protect Americans' privacy (obtaining a warrant or minimization by purging the record from the database), it does so not only after the communications is acquired but only after an analyst reviews the acquired communication. If a government analyst reviewed the communications and determined that "it was a U.S. person inside the United States . . . that would stimulate the system to get a warrant. And that is how the process would work." In other words, the NSA only seeks a warrant (if at all), after the communication is (1) illegally intercepted and acquired; (2) illegally placed in a government database; (3) illegally reviewed by an analyst; and (4) the system flags it for a warrant.

79. Under the Spying Program, the NSA engages in "electronic surveillance" as defined by FISA.

80. Under the Spying Program, the NSA engages in "interception" of both "wire communication[s]" and "electronic communication[s]" as defined in the Wiretap Act. 18 U.S.C. § 2510.

81. Under the Spying Program, the NSA intentionally accesses electronic communications without authorization and/or exceeds authorization to access electronic communications that are maintained in "electronic storage" as defined by the SCA.

82. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance both domestic and international telephone communications of people inside the United States, including citizens and lawful permanent residents, including plaintiffs.

83. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance both domestic and international Internet communications, including email, of people inside the United States, including citizens and lawful permanent residents, including plaintiffs, who are innocent, law-abiding citizens have no connection whatsoever to terrorism.

84. Under the Spying Program, the NSA has intercepted, subjected to electronic surveillance, and searched and seized millions of both domestic and international telephone and Internet communications (hereinafter collectively "communications") of people inside the United States, including citizens and lawful permanent residents, including plaintiffs. This includes the private phone conversations, private email, and private Internet use of millions of Americans.

85. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of people inside the United States without probable cause to believe that the surveillance targets have committed or are about to commit any crime.

86. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of people inside the United States without probable cause, reasonable suspicion, or any reason to believe that the surveillance targets either have committed or are about to commit any crime or are foreign powers or agents thereof.

87. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of people inside the United States without obtaining specific authorization for each interception from the President or the Attorney General.

88. Under the Spying Program, NSA shift supervisors are authorized to approve NSA employees' requests to intercept, search and seize, and subject to electronic surveillance the communications of people inside the United States.

89. Under the Spying Program, the NSA does not seek judicial review, obtain a search warrant, a court order, or any lawful authorization whatsoever before or after intercepting, searching and seizing, and subjecting to electronic surveillance the communications of people inside the United States.

90. On information and belief, pursuant to the secret Spying Program, the NSA has intercepted, searched and seized, and subjected to electronic surveillance private communications between Americans and their husbands, wives, children, parents, friends, pastors, doctors, lawyers, accountants, and others.

91. Each of the named plaintiffs was, pursuant to the Spying Program, subject to the unlawful interception, search and seizure, and electronic surveillance of the contents of their phone and Internet communications.

92. Prior to its initiation, defendants never advocated that Congress enact a bill authorizing the illegal Spying Program.

93. Prior to its initiation, defendants never sought authorization from the FISA Court to conduct the Spying Program.

94. Prior to its initiation, defendants never sought authorization from any Article III Court to conduct the Spying Program.

95. Defendants were, or should have been, well aware that the Spying Program was a clear violation of the law.

96. Defendants were, or should have been, well aware that the Spying Program is a federal crime.

Recognition of the Blatant Illegality of the Spying Program, and Continued Operations

97. The Spying Program was so blatantly illegal that, "when the presidential order was set to expire, the Department of Justice, under Acting Attorney General James Comey, refused to give its approval to the reauthorization of the order because of concerns about the legal basis of certain of these NSA activities." When the-then White House Counsel and Chief of Staff sought approval from Attorney General Ashcroft from his hospital bed, "Ashcroft gave a lucid account of the reasons that Justice had decided to withhold support. And then he went beyond that. Ashcroft said he never should have certified the program. Ashcroft specified a list of facts, and a list of legal concerns, that the secrecy rules had prevented him from discovering. Had he known them, he said, he would have withheld his signature before."

98. Despite the apparent conclusion by the Department of Justice that the Program violated criminal laws, President Bush nevertheless reissued the Program Order on or around March 11, 2004. As one author has explained, "Addington deleted the Justice Department from the document [and] typed in 'Alberto R. Gonzales,' the White House Counsel, on a substitute signature line. . . . He did not stop at adding a legally meaningless signature line for Gonzales. Addington drew up new language in which Bush relied upon his own authority to certify the program as lawful." As a result of this incident, about "two dozen Bush appointees," including Acting Attorney General Comey and FBI Director Mueller, were prepared to resign.

99. The Spying Program was so blatantly illegal that at least a dozen government officials with knowledge of the Program felt compelled as whistleblowers to report defendants' illegal conduct to *The New York Times*, notwithstanding substantial risks to their employment and potentially to their liberty.

100. After the revelations to *The New York Times*, defendant Bush authorized a criminal investigation into the whistleblowing activity.

101. To plaintiffs' knowledge, however, defendants have failed to open any criminal investigation into the Spying Program itself.

102. In August 2007, Congress passed the Protect America Act of 2007, Public Law 110-55 ("PAA"). Although not authorized by the PAA, the Spying Program continues to this day. As *The Wall Street Journal* noted in March 2008, the essential aspects of the Spying Program are unchanged: "According to current and former intelligence officials, the [NSA] now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records. The NSA receives this so-called 'transactional' data from other agencies or private companies, and its sophisticated software programs analyze the various transactions for suspicious patterns."

FIRST CAUSE OF ACTION

Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810

(against all Defendants)

103. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

104. Plaintiffs are "aggrieved person[s]" as defined in 50 U.S.C. § 1810, are not foreign powers or agents of a foreign power, and were subjected to electronic surveillance conducted or authorized by defendants pursuant to the Spying Program in violation of 50 U.S.C. § 1809.

105. Defendants are "person[s]" within 50 U.S.C. § 1801(m).

106. Plaintiffs are entitled to the damages set forth in 50 U.S.C. § 1810.

SECOND CAUSE OF ACTION

Wiretap Act, 18 U.S.C. §§ 2510, et seq.

(against Defendants Alexander, Hayden, Gonzales and Ashcroft)

107. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

108. Plaintiffs are "aggrieved person[s]" as defined in 18 U.S.C. § 2510.

109. The contents of plaintiffs' wire and electronic communications were intercepted by defendants pursuant to the Spying Program in violation of 18 U.S.C. § 2511.

110. Plaintiffs are entitled to the damages set forth in 18 U.S.C. § 2520.

THIRD CAUSE OF ACTION

Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*

(against Defendants Alexander, Hayden, Gonzales and Ashcroft)

111. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

112. Plaintiffs are "aggrieved" within 18 U.S.C. § 2707(a).

113. Defendants intentionally accessed plaintiffs' stored communications without authorization pursuant to the Spying Program in violation of 18 U.S.C. § 2701.

114. Plaintiffs are entitled to the damages set forth in 18 U.S.C. § 2707(c).

FOURTH CAUSE OF ACTION

Bivens/Fourth Amendment

(against all Individual Defendants)

115. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

116. By conducting, authorizing, and/or participating in the electronic surveillance of plaintiffs, and by searching and seizing the contents of plaintiffs' communications without reasonable suspicion or probable cause, and failing to prevent their fellow government officers from engaging in this unconstitutional conduct, defendants deprived plaintiffs of rights, remedies, privileges, and immunities guaranteed under the Fourth Amendment of the United States Constitution.

117. In addition, defendants conspired among themselves to deprive plaintiffs of their Fourth Amendment rights, and took numerous overt steps in furtherance of such conspiracy, as set forth above.

118. As a direct and proximate result of the misconduct and abuse of authority detailed above, plaintiffs sustained a shocking loss of privacy, and the damages hereinbefore alleged.

WHEREFORE, plaintiffs respectfully seek:

(A) an order certifying this action as a class action pursuant to Fed. R. Civ. P. 23(b) for the plaintiff class described herein and naming plaintiffs as the class representatives;

(B) a judgment declaring that defendants' Spying Program violates FISA, the Wiretap Act, SCA, and the Fourth Amendment, and permanently enjoining the Spying Program or any NSA electronic surveillance of United States persons without a search warrant or court order, and requiring defendants to delete and destroy, permanently and irrevocably, every communication and record of every communication intercepted by the NSA pursuant to the Spying Program in the custody, control, or possession of the United States or any of its agents or employees;

(C) an award of liquidated and/or compensatory damages to the named plaintiffs and members of the class in an amount to be determined at trial;

(D) an award of punitive damages to the named plaintiffs and members of the class against the individual defendants in an amount to be determined at trial;

(E) an award of reasonable attorneys' fees, costs, and disbursements, pursuant to 50 U.S.C. § 1810, 18 U.S.C. § 2520, 18 U.S.C. § 2707, and 28 U.S.C. § 2412.

(F) a grant of such other and further relief as this Court shall find just and proper.

Dated: May 8, 2012

EMERY CELLI BRINCKERHOFF & ABADY LLP

By: _____
Ilann M. Maazel
Matthew D. Brinckerhoff
Adam R. Pulver

75 Rockefeller Plaza, 20th Floor
New York, N.Y. 10019
Phone: (212) 763-5000
Fax: (212) 763-5001

Attorneys for Plaintiffs