PETER D. KEISLER
Assistant Attorney General
CHRISTOPHER J. CHRISTIE
United States Attorney
SUSAN STEELE
Assistant United States Attorney
CARL J. NICHOLS
Deputy Assistant Attorney General
DOUGLAS LETTER
Terrorism Litigation Counsel
ARTHUR R. GOLDBERG
Assistant Director, Federal Programs Branch
ALEXANDER HAAS
Trial Attorney, Federal Programs Branch
UNITED STATES DEPARTMENT OF JUSTICE
P.O. BOX 883
WASHINGTON, DC 20044
(202) 307-3937

BY: IRENE DOWDY
Assistant United States Attorney
(609) 989-0562

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

THE UNITED STATES OF AMERICA, Plaintiff, v. ZULIMA V. FARBER, in her official capacity as Attorney General of the State of New Jersey; CATHLEEN O'DONNELL, in her official capacity as Deputy Attorney General of the State of New Jersey; KIMBERLY S. RICKETTS, in her official capacity as Director of the New Jersey Division of Consumer Affairs; AT&T CORP.; VERIZON COMMUNICATIONS INC; QWEST COMMUNICATIONS INTERNATIONAL, INC.; SPRINT NEXTEL CORPORATION; and CINGULAR WIRELESS LLC, Defendants.	CIVIL ACTION NO.: COMPLAINT

Plaintiff, the United States of America, by its undersigned attorneys, brings this civil action for declaratory and injunctive relief, and alleges as follows:

INTRODUCTION

1. In this action, the United States seeks to prevent the disclosure of highly confidential and sensitive government information that the defendant officers of the State of New Jersey have sought to obtain from telecommunications carriers without proper authorization from the United States. Compliance with the subpoenas issued by those officers would first place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without causing exceptionally grave harm to national security. And if particular carriers are indeed supplying foreign intelligence information to the Federal Government, compliance with the subpoenas would require disclosure of the details of that activity. The defendant state officers' attempts to obtain such information are invalid under the Supremacy Clause of the United States Constitution and are preempted by the United States Constitution and various federal statutes. This Court should therefore enter a declaratory judgment that the State Defendants do not have the authority to seek confidential and sensitive federal government information and thus cannot enforce the subpoenas they have served on the telecommunications carriers.

JURISDICTION AND VENUE

2. The Court has jurisdiction pursuant to 28 U.S.C. §§ 1331, 1345.

3. Venue lies in the District of New Jersey pursuant to 28 U.S.C. § 1391(b)(1) and (2).

PARTIES

4. Plaintiff is the United States of America, suing on its own behalf.

5. Defendant Zulima V. Farber is the Attorney General for the State of New Jersey, and maintains her offices in Mercer County. She is being sued in her official capacity.

6. Defendant Cathleen O'Donnell is the Deputy Attorney General for the State of New Jersey, and maintains her offices in Mercer County. She is being sued in her official capacity.

7. Defendant Kimberly S. Ricketts is the Director of the New Jersey Division of Consumer Affairs. She is being sued in her official capacity. Defendants Zulima V. Farber, Cathleen O'Donnell, and Kimberly S. Ricketts are referred to as the "State Defendants."

8. Defendant AT&T Corp. is a corporation incorporated in the state of New York with its principal place of business in Somerset County, New Jersey, and that has received a subpoena in New Jersey.

9. Defendant Verizon Communications Inc. is a corporation incorporated in the state of Delaware with its principal place of business in the state of New York, that has offices in Somerset County, New Jersey, and that has received a subpoena in New Jersey.

10. Defendant Qwest Communications International, Inc. is a corporation incorporated in the state of Delaware with its principal place of business in the state of Colorado, and that has received a subpoena in New Jersey.

11. Defendant Sprint Nextel Corporation is a corporation incorporated in the state of New Jersey with its principal place of business in the state of Virginia, and that has received a subpoena in New Jersey.

12. Defendant Cingular Wireless LLC is a corporation incorporated in the state of Delaware with its principal place of business in Georgia, and that has received a subpoena in

New Jersey.

13. Defendants AT&T Corp., Cingular Wireless LLC, Qwest Communications International, Inc., Sprint Nextel Corporation, and Verizon Communications, Inc. are referred to as the "Carrier Defendants."

STATEMENT OF THE CLAIM

I. The Federal Government Has Exclusive Control Vis-a-Vis the States With Respect to Foreign-Intelligence Gathering, National Security, the Conduct of Foreign Affairs, and the Conduct of Military Affairs.

14. The Federal Government has exclusive control vis-a-vis the States over foreign-intelligence gathering, over national security, and over the conduct of war with foreign entities. The Federal Government controls the conduct of foreign affairs, the conduct of military affairs, and the performance of the country's national security function.

15. In addition, various federal statutes and Executive Orders govern and regulate access to information relating to foreign intelligence gathering.

16. For example, Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1), confers upon the Director of National Intelligence the authority and responsibility to "protect intelligence sources and methods from unauthorized disclosure."

17. Federal law also makes it a felony for any person to divulge classified information "concerning the communication intelligence activities of the United States" to any person who has not been authorized by the President, or his lawful designee, to receive such information. 18 U.S.C. § 798.

18. And federal law establishes unique protections from disclosure for information related to the National Security Agency. Federal law states that "nothing in this . . . or any other

law . . . shall be construed to require disclosure of . . . any function of the National Security Agency, [or] of any information with respect to the activities thereof." 50 U.S.C. § 402 note.

19. Several Executive Orders have been promulgated pursuant to these constitutional and statutory authorities that govern access to and handling of national security information.

20. First, Executive Order No. 12958, 60 Fed. Reg. 19825 (April 17, 1995), as amended by Executive Order No. 13292, 68 Fed. Reg. 15315 (March 25, 2003), prescribes a uniform system for classifying, safeguarding and declassifying national security information. It provides that:

> A person may have access to classified information provided that:
>
> (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
>
> (2) the person has signed an approved nondisclosure agreement; and
>
> (3) the person has a need-to-know the information.

Exec. Order No. 13292, Sec. 4.1(a). "Need-to-know" means "a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." Exec. Order No. 12958, Sec. 4.1(c). Executive Order No. 12958 further states, in part, that "Classified information shall remain under the control of the originating agency or its successor in function." Exec. Order No. 13292, Sec. 4.1(c).

21. Second, Executive Order No. 12968, 60 Fed. Reg. 40245 (Aug. 2, 1995), establishes a uniform Federal personnel security program for employees of the Federal Government, as well as employees of an industrial or commercial contractor of a Federal agency, who will be considered for initial or continued access to the classified information. The Order states, in part,

that "Employees who are granted eligibility for access to classified information shall . . . protect classified information in their custody from unauthorized disclosure . . . ." Exec. Order No. 12968, Sec. 6.2(a)(1).

22. In addition, the courts have developed several doctrines that are relevant to this dispute and that establish the supremacy of federal law with respect to national security information and intelligence gathering. For example, suits alleging secret espionage agreements with the United States are not justiciable.

23. The Federal Government also has an absolute privilege to protect military and state secrets from disclosure. Only the Federal Government can waive that privilege, which is often called the "state secrets privilege."

II. The Terrorist Surveillance Program and the Federal Government's Invocation of the State Secrets Privilege

24. The President has explained that, following the devastating events of September 11, 2001, he authorized the National Security Agency ("NSA") to intercept certain international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. *See* Press Conference of President Bush (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html. ("President's Press Release").

25. The Attorney General of the United States has further explained that, in order to intercept a communication, there must be "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005),

available at http://whitehouse.gov/news/releases/2005/12/20051219-1.html. This activity is known as the Terrorist Surveillance Program ("TSP").

26. The purpose of these intercepts is to provide the United States with an early warning system to detect and prevent another catastrophic terrorist attack in the United States. *See* President's Press Release. The President has stated that the NSA activities "ha[ve] been effective in disrupting the enemy, while safeguarding our civil liberties." *Id.*

27. Since January 2006, more than 20 class action lawsuits have been filed alleging that telecommunications carriers, including the Carrier Defendants, have unlawfully provided assistance to the NSA. The first lawsuit, *Hepting v. AT&T Corp., et al.*, was filed in the District Court for the Northern District of California in January 2006. Case No. C-06-0672-VRW.

28. Those lawsuits, including the *Hepting* case, generally make two sets of allegations. First, the lawsuits allege that the telecommunications carriers unlawfully intercepted the contents of certain telephone calls and emails and provided them to the NSA. Second, the lawsuits allege that telecommunications carriers have unlawfully provided the NSA with access to calling records and related information.

29. The Judicial Panel on Multidistrict Litigation is currently considering a motion to transfer all of these lawsuits to a single district court for pretrial proceedings. *In re: National Security Agency Telecommunications Records Litigation*, MDL Docket No. 1791 (JPML).

30. In the *Hepting* case, the state secrets privilege has been formally asserted by the Director of National Intelligence, John D. Negroponte, and the Director of the National Security Agency, Lieutenant General Keith B. Alexander. The Director of National Intelligence is the "head of the intelligence community" of the United States. 50 U.S.C. § 403(b)(1). General Alexander has also invoked the NSA's statutory privilege. *See* 50 U.S.C. § 402 note.

31. The public declarations of the Director of National Intelligence and the Director of the NSA in the *Hepting* case state that, "[i]n an effort to counter the al Qaeda threat, the President of the United States authorized the NSA to utilize its [signals intelligence] capabilities to collect certain 'one-end foreign' communications where one party is associated with the al Qaeda terrorist organization for the purpose of detecting and preventing another terrorist attack on the United States. This activity is known as the Terrorist Surveillance Program ('TSP')." Negroponte Decl. ¶ 11 (Exhibit A, attached to this Complaint); *see* Alexander Decl. ¶ 7 (Exhibit B, attached to this Complaint).

32. Director Negroponte and General Alexander have concluded that "[t]o discuss this activity in any greater detail, however, would disclose classified intelligence information and reveal intelligence sources and methods, which would enable adversaries of the United States to avoid detection by the U.S. Intelligence Community and/or take measures to defeat or neutralize U.S. intelligence collection, posing a serious threat of damage to the United States' national security interests." Negroponte Decl. ¶ 11; *see* Alexander Decl. ¶ 7.

33. The public declarations further state that "any further elaboration on the public record concerning these matters would reveal information that could cause the very harms [that] the assertion of the state secrets privilege is intended to prevent." Negroponte Decl. ¶ 12; *see* Alexander Decl. ¶ 8. The assertion of the privilege encompasses "allegations about NSA's purported involvement with AT&T." Negroponte Decl. ¶ 12; Alexander Decl. ¶ 8. Director Negroponte and General Alexander have explained that "[t]he only recourse for the Intelligence Community and, in this case, for the NSA, is to neither confirm nor deny these sorts of allegations, regardless of whether they are true or false. To say otherwise when challenged in

litigation would result in routine exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general." Negroponte Decl. ¶ 12; *see* Alexander Decl. ¶ 8.

III. The State Defendants Seek to Require the Production of Potentially Highly Classified and Sensitive Information

34. On May 17, 2006, the State Defendants sent subpoenas duces tecum entitled "Provision of Telephone Call History Data to the National Security Agency" ("Subpoenas") to each of the Carrier Defendants. A representative Subpoena is attached as Exhibit C. The materials sought by these Subpoenas include, among other items, "[a]ll names and complete addresses of Persons including, but not limited to, all affiliates, subsidiaries and entities, that provide Telephone Call History Data to the NSA";[1] "[a]ll Executive Orders issued by the President of the United States and provided to Verizon concerning any demand or request to provide Telephone Call History Data to the NSA"; "[a]ll orders, subpoenas and warrants issued by or on behalf of any unit or officer of the Executive Branch of the Federal Government and provided to Verizon concerning any demand or request to provide Telephone Call History Data to the NSA"; "[a]ll orders, subpoenas and warrants issued by or on behalf of any Federal or State judicial authority and provided to Verizon concerning any demand or request to provide Telephone Call History Data to the NSA"; "[a]ll Documents concerning the basis for Verizon's provision of Telephone Call History Data to the NSA, including, but not limited to, any legal or contractual authority"; "[a]ll Documents concerning any written or oral contracts, memoranda of

[1] Under the Subpoenas, "'Telephone Call History Data' means any data Verizon provided to the NSA including, but not limited to, records of landline and cellular telephone calls placed, and/or received by a Verizon subscriber with a New Jersey billing address or New Jersey telephone number." See Definitions, ¶ 8.

understanding, memoranda of agreement, other agreements or correspondence by or on behalf of Verizon and the NSA concerning the provision of Telephone Call History Data to the NSA"; "[a]ll Documents concerning any communication between Verizon and the NSA or any other unit or officer of the Executive Branch of the Federal Government concerning the provision of Telephone Call History Data to the NSA"; and "[t]o the extent not otherwise requested, [a]ll Documents concerning any demand or request that Verizon provide Telephone Call History Data to the NSA." See Subpoenas, ¶¶ 1-13.

35. These Subpoenas specify that they are "issued pursuant to the authority of N.J.S.A. 56:8-1, et seq., specifically N.J.S.A. 56:8-3 and 56:8-4." The cited provisions of state law concern consumer fraud, and provide, *inter alia*, that "[w]hen it shall appear to the [state] Attorney General that a person has engaged in, is engaging in, or is about to engage in any practice declared to be unlawful by this act, or when he believes it to be in the public interest that an investigation should be made to ascertain whether a person in fact has engaged in, is engaging in or is about to engage in, any such practice, he may . . . [e]xamine any merchandise or sample thereof, record, book, document, account or paper as he may deem necessary." N.J.S.A. 56:8-3. "To accomplish the objectives and to carry out the duties prescribed by this act, the [state] Attorney General, in addition to other powers conferred upon him by this act, may issue subpoenas to any person, administer an oath or affirmation to any person, conduct hearings in aid of any investigation or inquiry, promulgate such rules and regulations, and prescribe such forms as may be necessary, which shall have the force of law." N.J.S.A. 56:8-4.

36. The cover letter accompanying these Subpoenas states: "Failure to comply with this Subpoena may render you liable for contempt of court and such other penalties as are provided

by law."

37. These Subpoenas demand that responses be submitted by the Carrier Defendants on or before May 30, 2006. The State Defendants have extended the time for responses to June 15, 2006.

IV. The State Defendants Lack Authority to Compel Compliance with the Subpoenas.

38. The State Defendants' authority to seek or obtain the information requested in these Subpoenas is fundamentally inconsistent with and preempted by the Federal Government's exclusive control over all foreign intelligence gathering activities. In addition, no federal law authorizes the State Defendants to obtain the information they seek.

39. The State Defendants have not been granted access to classified information related to the activities of the NSA pursuant to the requirements set out in Executive Order No. 12958 or Executive Order No. 13292.

40. The State Defendants have not been authorized to receive classified information concerning the communication intelligence activities of the United States in accordance with the terms of 18 U.S.C. § 798, or any other federal law, regulation, or order.

41. In seeking information bearing upon NSA's purported involvement with the Carrier Defendants, the Subpoenas seek disclosure of matters with respect to which the Director of National Intelligence has determined that disclosure, including confirming or denying whether or to what extent such materials exist, would improperly reveal intelligence sources and methods.

42. The United States has a strong and compelling interest in preventing the disclosure of sensitive and classified information. The United States has a strong and compelling interest in preventing terrorists from learning about the methods and operations of terrorist surveillance

activities being undertaken or not being undertaken by the United States.

43. As a result of the Constitution, federal laws, applicable privileges, and the United States' interest in preventing the unauthorized disclosure of sensitive or classified information, the Carrier Defendants will be unable to confirm or deny their involvement, if any, in intelligence activities of the United States, and therefore cannot provide a substantive response to the Subpoenas.

44. The United States will be irreparably harmed if the Carrier Defendants are permitted or are required to disclose sensitive and classified information to the State Defendants in response to the Subpoenas.

COUNT ONE – VIOLATION OF AND PREEMPTION UNDER THE SUPREMACY CLAUSE AND FEDERAL LAW
(ALL DEFENDANTS)

45. Plaintiff incorporates by reference paragraphs 1 through 46 above.

46. The Subpoenas, and any responses required thereto, are invalid under, and preempted by, the Supremacy Clause of the United States Constitution, Art. VI, Cl. 2, federal law, and the Federal Government's exclusive control over foreign intelligence gathering activities, national security, the conduct of foreign affairs, and the conduct of military affairs.

COUNT TWO – UNAUTHORIZED DISCLOSURE OF SENSITIVE AND CONFIDENTIAL INFORMATION
(ALL DEFENDANTS)

47. Plaintiff incorporates by reference paragraphs 1 through 48 above.

48. Providing responses to the Subpoenas would be inconsistent with and would violate federal law including, but not limited to, Executive Order 12958, 18 U.S.C. § 798, and 50 U.S.C. § 402 note, as well as other applicable federal laws, regulations, and orders.

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays for the following relief:

1. That this Court enter a declaratory judgment pursuant to 28 U.S.C. § 2201(a), that the Subpoenas issued by the State Defendants may not be enforced by the State Defendants or responded to by the Carrier Defendants because any attempt to obtain or disclose the information that is the subject of the these Subpoenas would be invalid under, preempted by, and inconsistent with the Supremacy Clause of the United States Constitution, Art. VI, Cl. 2, federal law, and the Federal Government's exclusive control over foreign intelligence gathering activities, national security, the conduct of foreign affairs, and the conduct of military affairs.

2. That this Court grant plaintiff such other and further relief as may be just and proper, including any necessary and appropriate injunctive relief.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General
CHRISTOPHER J. CHRISTIE
United States Attorney
SUSAN STEELE
Assistant United States Attorney
CARL J. NICHOLS
Deputy Assistant Attorney General
DOUGLAS LETTER
Terrorism Litigation Counsel
ARTHUR R. GOLDBERG
Assistant Director, Federal Programs Branch
ALEXANDER HAAS
Trial Attorney, Federal Programs Branch
U.S. DEPARTMENT OF JUSTICE
P.O. BOX 883
WASHINGTON, DC 20044
(202) 307-3937

/s/

BY: IRENE DOWDY
Assistant United States Attorney
(609) 989-0562

DATED: Trenton, New Jersey
June 14, 2006