Alexander W. Moore
Associate General Counsel – New England

verizon

185 Franklin Street
13th Floor
Boston, MA 02110-1585

Phone 617 743-2265
Fax 617 737-0648
alexander.w.moore@verizon.com

August 30, 2006

Thomas F. Ahern, Administrator
Division of Public Utilities and Carriers
89 Jefferson Boulevard
Warwick, RI 02888

Re: Rhode Island American Civil Liberties Union Informal Complaint
Docket No. D-06-45

Dear Mr. Ahern:

By way of supplement to my letter to you of June 16, 2006, in the above matter, enclosed herewith are copies of the Complaint and related exhibits in *United States v. Adams, et al.,* a suit the United States filed against the Maine Public Utilities Commission and Verizon New England on August 21, 2006, to prevent disclosure by Verizon of information sought by that Commission concerning allegations that Verizon had disclosed records to the National Security Administration, similar to allegations the ACLU–RI has made to the Division.

Sincerely,

Alexander W. Moore/msl

Alexander W. Moore

Enclosures
cc: Ms. Donna Cupelo
Mr. Steven Brown
Service List

UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

THE UNITED STATES OF AMERICA, Plaintiff, v. KURT ADAMS, in his official capacity as Chairman of the Maine Public Utilities Commission; SHARON M. REISHUS, in her official capacity as Commissioner of the Maine Public Utilities Commission; DENNIS L. KESCHL in his official capacity as Acting Administrative Director of the Maine Public Utilities Commission; VERIZON NEW ENGLAND INC. D/B/A VERIZON MAINE 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 Maine Public Utilities Commission ("MPUC") have sought to obtain from Verizon New England Inc. d/b/a Verizon Maine ("Verizon") without proper authorization from the United States. Compliance with the August 9, 2006 Order of the MPUC (the "Order") or other similar order issued by those officers would first place Verizon 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 telecommunication carriers are indeed supplying foreign intelligence information to the Federal Government, compliance with the Order or other similar order 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.

JURISDICTION AND VENUE

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

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

PARTIES

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

5. Defendant Kurt Adams is the Chairman of the Maine Public Utilities Commission, and maintains his offices in Kennebec County. He is being sued in his official capacity.

6. Defendant Sharon M. Reishus is a Commissioner on the Maine Public Utilities Commission, and maintains her offices in Kennebec County. She is being sued in her official capacity.

7. Defendant Dennis L. Keschl is Acting Administrative Director of the Maine Public Utilities Commission and maintains his offices in Kennebec County. He is being sued in his official capacity.

8. Defendant Verizon New England Inc. d/b/a Verizon Maine ("Verizon") is a New York corporation with a principal place of business in Boston, Massachusetts and that has offices at One Davis Farm Road, Portland, Maine, and has received a copy of the August 9, 2006 Order.

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.

9. 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.

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

11. 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."

12. 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.

13. 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.

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

15. 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).

16. 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).

17. 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.

18. 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. Alleged NSA Activities and the Federal Government's Invocation of the State Secrets Privilege

19. On May 11, 2006, USA Today published an article alleging that the NSA has been secretly collecting the phone call records of millions of Americans from various telecommunications carriers. The article reported on the purported activities of telecommunications carriers. No United States official has confirmed or denied the existence of the alleged program subject to the USA Today article. Unclassified Declaration of Keith B. Alexander in *Terkel v. AT&T, et al.*, ("Alexander Decl.") ¶ 8 (Exhibit A, attached to this Complaint).

20. Since January 2006, more than 30 class action lawsuits have been filed alleging that telecommunications carriers, including Verizon, 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.

21. 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.

22. The Judicial Panel on Multidistrict Litigation granted a motion to transfer all of these lawsuits to a single district court for pretrial proceedings on August 9, 2006. *In re: National Security Agency Telecommunications Records Litigation*, MDL Docket No. 1791 (JPML).

23. In both the *Hepting* and *Terkel v. AT&T, et al.*, 06-cv-2837 (MFK) (N.D. Il.), cases, 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.

24. As in the *Terkel* case, where the United States invoked the state secrets privilege, the MPUC's August 9, 2006 Order seeks information in an attempt to confirm or deny the existence of alleged intelligence-gathering activities.

25. In *Terkel*, Director Negroponte stated that "the United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets" and that "[t]he harm of revealing such information should be obvious" because "[i]f the United States confirms that it is conducting a particular intelligence activity, that it is gathering information from a particular source, or that it has gathered information on a particular person, such intelligence-gathering activities would be compromised and foreign adversaries such as al Qaeda and affiliated terrorist organizations could use such information to avoid detection." *See* Unclassified Declaration of John D. Negroponte in *Terkel* ("Negroponte Decl.") ¶ 12 (Exhibit B, attached to this Complaint). Furthermore, "[e]ven confirming that a certain intelligence activity or relationship does *not* exist, either in general or with respect to specific targets or channels,

would cause harm to the national security because alerting our adversaries to channels or individuals that are not under surveillance could likewise help them avoid detection." *Id.* Director Negroponte went on to explain that "if the government, for example, were to confirm in certain cases that specific intelligence activities, relationships, or targets do not exist, but then refuse to comment (as it would have to) in a case involving an actual intelligence activity, relationship, or target, a person could easily deduce by comparing such responses that the latter case involved an actual intelligence activity, relationship, or target." *Id.* In light of the exceptionally grave damage to national security that could result from any such information, both Director Negroponte and General Alexander have explained that "[a]ny further elaboration on the public record concerning these matters would reveal information that would cause the very harms that my assertion of privilege is intended to prevent." *Id.*; *see* Alexander Decl. ¶ 7.

26. The assertion of the state secrets privilege in *Terkel* and the privilege of the National Security Agency therefore covered "any information tending to confirm or deny (a) alleged intelligence activities, such as the alleged collection by the NSA of records pertaining to a large number of telephone calls, (b) an alleged relationship between the NSA and AT&T (either in general or with respect to specific alleged intelligence activities), and (c) whether particular individuals or organizations have had records of their telephone calls disclosed to the NSA." Negroponte Decl. ¶ 11; *see* Alexander Decl. ¶¶ 7-8. In other words, the state secrets privilege covers precisely the same types of information that the State Defendants seek from Verizon.

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

27. The MPUC proceeding began on May 8, 2006, when a complaint was filed by James D. Cowie requesting that the MPUC open an investigation into whether Verizon, in Maine, was

aiding the NSA in an alleged wiretapping program. Verizon sought to dismiss the complaint by, *inter alia*, noting that federal law prohibited providing specific information regarding Verizon's alleged cooperation, or lack thereof, with the NSA. Verizon also noted that this matter could not be reviewed by the MPUC.

28. The MPUC itself recognizes that federal law limits its authority to seek information regarding alleged intelligence-gathering activities. The MPUC issued a Procedural Order on June 23, 2006, that recognized the "more difficult issue" of "whether certain federal statutes and/or the so-called 'state secrets privilege' will prevent [the MPUC] from obtaining relevant information in the course of a Commission investigation." The Department of Justice subsequently advised the MPUC that any attempts to obtain information from the telecommunication carriers could not be accomplished without harming national security, and responses would be inconsistent with federal law. The Department of Justice also advised the MPUC that its authority to obtain information in this instance is preempted by federal law *See* Letter of July 28, 2006, from Peter D. Keisler to Chairman Adams and Commissioner Reishus, attached as Exhibit C (without enclosures).

29. Nevertheless, on August 9, 2006, the State Defendants issued the Order that, among other things, seeks to "require that Verizon provide sworn affirmations of representations it made in its filed response to the complaint." A copy of the August 9, 2006 Order is attached as Exhibit D.

30. This August 9, 2006 Order specifies that it was issued "[p]ursuant to our authority set forth in 35-A M.R.S.A. § 112(2)." Exhibit D at 3. The cited provisions of state law provide, *inter alia*, that the Commission has the power to investigate the management of the business of all public utilities. Me. Rev. Stat. Ann. tit. 35-A, § 112(1). Other provisions provide that

"[e]very public utility shall furnish the commission . . . [a]ll information necessary to perform its duties and carry into effect this Title," *id.* § 112(2), that the Commission "by order or subpoena" may require the utility to produce documents. *Id.* § 112(4). If a public utility or person fails to comply with an order, decision, rule, direction, demand, or requirement of the Commission, that entity is in contempt of the Commission. Me. Rev. Stat. Ann. 35-A, § 1502.

31. The Order demands that responses be submitted by Verizon on or before August 21, 2006. Exhibit D at 4. Defendants issued this Order notwithstanding being advised by the Department of Justice on July 28, 2006, that the MPUC's attempts to require telecommunication carriers to provide information would be inconsistent with, and preempted by, federal law. *See* Exhibit C. Indeed, a comprehensive body of federal law governs the field of foreign intelligence gathering and bars any unauthorized disclosures as contemplated by this Order, thereby preempting state law, including: (i) Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note; (ii) 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); and (iii) 18 U.S.C. § 798(a).

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

32. The State Defendants' attempts to seek or obtain the information requested in the August 9, 2006 Order, as well as any related information, are 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.

33. 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.

34. 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.

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

36. 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.

37. 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, Verizon will be unable to confirm or deny their involvement, if any, in intelligence activities of the United States.

38. The United States will be irreparably harmed if Verizon is permitted or is required to disclose sensitive and classified information to the State Defendants.

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

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

40. The State Defendants attempts to procure the information sought through the Order,

or any other related information, 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.

41. The State Defendants attempts to procure the information sought through the Order, or any other related information, and any responses required thereto, are also invalid because the no organ of State government, such as the Maine Public Utilities Commission, or its officers, may regulate or impede the operations of the federal government under the Constitution.

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

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

43. Providing responses to the Order or other similar orders 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 State Defendants may not enforce the Order or otherwise seek information pertaining to alleged foreign intelligence functions of the federal government and that Verizon may not provide such information, because any attempt to obtain or disclose such information 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.

Dated: August 21, 2006

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

PAULA D. SILSBY
United States Attorney

CARL J. NICHOLS
Deputy Assistant Attorney General

DOUGLAS LETTER
Terrorism Litigation Counsel

ARTHUR R. GOLDBERG
Assistant Director, Federal Programs Branch

/s/ Alexander K. Haas
ALEXANDER K. HAAS
Trial Attorney, Federal Programs Branch
UNITED STATES DEPARTMENT OF JUSTICE
P.O. BOX 883
WASHINGTON, DC 20044
(202) 307-3937

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

STUDS TERKEL, BARBARA FLYNN CURRIE, DIANE C. GERAGHTY, GARY S. GERSON JAMES D. MONTGOMERY, and QUENTIN YOUNG, on behalf of themselves and all others similarly situated, and the AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS,	)	Case No. 06 C 2837
Plaintiffs,	)	Hon. Matthew F. Kennelly
v.	)	
AT&T INC., AT&T CORP., and ILLINOIS BELL TELEPHONE CO. d/b/a AT&T ILLINOIS,	)	
Defendants.	)	

DECLARATION OF LIEUTENANT GENERAL KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY

I, Keith B. Alexander, declare as follows:

INTRODUCTION

1. I am the Director of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for directing the NSA, overseeing the operations undertaken to carry out its mission and, by specific charge of the President and the Director of National Intelligence, protecting NSA activities and intelligence sources and methods. I have been designated an original TOP SECRET classification authority under Executive Order No. 12958, 60 Fed. Reg. 19825 (1995), as amended on March 25, 2003, and Department of Defense Directive No. 5200.1-R, Information Security Program Regulations, 32 C.F.R. § 159a.12 (2000).

2. The purpose of this declaration is to support the assertion of a formal claim of the military and state secrets privilege (hereafter "state secrets privilege"), as well as a statutory

privilege, by the Director of National Intelligence (DNI), John D. Negroponte, as the head of the U.S. Intelligence Community. In this declaration, I also assert a statutory privilege with respect to information about NSA activities. For the reasons described below, and in my classified declaration provided separately to the Court for *in camera* and *ex parte* review, the disclosure of the information covered by these privilege assertions would cause exceptionally grave damage to the national security of the United States. The statements made herein, and in my classified declaration, are based on my personal knowledge of NSA operations and on information made available to me as Director of the NSA.

THE NATIONAL SECURITY AGENCY

3. The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. Under Exec. Order 12333, § 1.12.(b), as amended, NSA's cryptologic mission includes three functions: (1) to collect, process, and disseminate signals intelligence ("SIGINT") information, of which communications intelligence ("COMINT") is a significant subset, for (a) national foreign intelligence purpose, (b) counterintelligence purposes, and (c) the support of military operations; (2) to conduct information security activities; and (3) to conduct operations security training for the U.S. Government.

4. There are two primary reasons for gathering and analyzing intelligence information. The first, and most important, is to gain information required to direct U.S. resources as necessary to counter external threats. The second reason is to obtain information necessary to the formulation of the United States' foreign policy. Foreign intelligence information provided by NSA is thus relevant to a wide range of important issues, including military order of battle; threat warnings and readiness; arms proliferation; terrorism; and foreign aspects of international narcotics trafficking.

5. In the course of my official duties, I have been advised of this litigation and the allegations at issue. As described herein and in my separate classified declaration, information implicated by Plaintiffs' claims is subject to the state secrets privilege assertion in this case by the DNI. The disclosure of this information would cause exceptionally grave damage to the national security of the United States. In addition, it is my judgment that any attempt to proceed in the case will substantially risk disclosure of the privileged information and will cause exceptionally grave damage to the national security of the United States.

6. Through this declaration, I also hereby invoke and assert NSA's statutory privilege to protect information related to NSA activities described below and in more detail in my classified declaration. NSA's statutory privilege is set forth in section 6 of the National Security Agency Act of 1959 (NSA Act), Public Law No. 86-36 (codified as a note to 50 U.S.C. § 402). Section 6 of the NSA Act provides that "[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency [or] any information with respect to the activities thereof. . . ." By this language, Congress expressed its determination that disclosure of any information relating to NSA activities is potentially harmful. Section 6 states unequivocally that, notwithstanding *any* other law, NSA cannot be compelled to disclose *any* information with respect to its authorities. Further, NSA is not required to demonstrate specific harm to national security when invoking this statutory privilege, but only to show that the information relates to its activities. Thus, to invoke this privilege, NSA must demonstrate only that the information to be protected falls within the scope of section 6. NSA's functions and activities are therefore protected from disclosure regardless of whether or not the information is classified.

INFORMATION SUBJECT TO CLAIMS OF PRIVILEGE

7. I support Director Negroponte's assertion of the state secrets privilege, and assert

NSA's statutory privilege with respect to any information tending to confirm or deny (a) alleged intelligence activities, such as the alleged collection by the NSA of records pertaining to a large number of telephone calls, (b) an alleged relationship between the NSA and AT&T (either in general or with respect to specific alleged intelligence activities), and (c) whether particular individuals or organizations have had records of their telephone calls disclosed to the NSA. I describe this information, and the exceptionally grave harm that would result from its disclosure, in further detail in my classified declaration. In his unclassified and classified declarations, Director Negroponte also describes the harms to the national security that would result from the disclosure of this information. Any further elaboration on the public record concerning these matters would reveal information that would cause the very harms that the assertion of the state secrets and statutory privileges is intended to prevent.

8. Moreover, it is my conclusion that the very subject matter of this action implicates privileged information. Plaintiffs allege, for example, that AT&T provides to the NSA records pertaining to the telephone calls of millions of AT&T customers, including themselves, and that such records are provided "in the absence of any warrant, court order, administrative subpoena, statutory authority, certification pursuant to the Act, customer consent, or any other lawful basis." Amended Compl. ¶¶ 1, 2. (Despite speculation in the media, such allegations have not been confirmed or denied by the United States.) Plaintiffs also seek, in their First Set of Interrogatories, information regarding whether AT&T has disclosed telephone records to the NSA pursuant to certain statutory provisions. Plaintiffs' claims cannot be litigated, or their Interrogatories answered, without the disclosure of privileged information—*i.e.*, information confirming or denying (a) an alleged intelligence activity, (b) an alleged relationship between the NSA and AT&T with respect to a specific alleged intelligence activity, and (c) whether records of Plaintiffs' telephone calls have been disclosed to the NSA.

Because the disclosure of such information would cause exceptionally grave damage to the national security, as described further in my classified declaration and Director Negroponte's classified and unclassified declarations, I respectfully request that this case be dismissed.

CONCLUSION

9. In sum, I support Director Negroponte's assertion of the state secrets privilege and statutory privilege, and I assert the NSA's statutory privilege, to prevent the disclosure of the information described generally herein and in the classified declarations available for the Court's *in camera* and *ex parte* review. Moreover, because proceedings in this case—including any proceeding or response related to Plaintiffs' Amended Complaint, Plaintiffs' Motion for a Preliminary Injunction, or Plaintiffs' First Set of Interrogatories—risk disclosure of privileged intelligence-related information, I respectfully request that the Court not only protect that information from disclosure, but also dismiss this case to stem the grave harms to the national security that will occur if this case proceeds.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: 30 June 06

LT. GEN. KEITH B. ALEXANDER
Director, National Security Agency

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

STUDS TERKEL, BARBARA FLYNN CURRIE, DIANE C. GERAGHTY, GARY S. GERSON JAMES D. MONTGOMERY, and QUENTIN YOUNG, on behalf of themselves and all others similarly situated, and the AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS,	)	Case No. 06 C 2837
	)	Hon. Matthew F. Kennelly
Plaintiffs,	)	
v.	)	
AT&T INC., AT&T CORP., and ILLINOIS BELL TELEPHONE CO. d/b/a AT&T ILLINOIS,	)	
Defendants.	)	

DECLARATION OF JOHN D. NEGROPONTE,
DIRECTOR OF NATIONAL INTELLIGENCE

I, John D. Negroponte, declare as follows:

INTRODUCTION

1. I am the Director of National Intelligence (DNI) of the United States. I have held this position since April 21, 2005. From June 28, 2004, until appointed to be DNI, I served as the United States Ambassador to Iraq. From September 18, 2001, until my appointment in Iraq, I served as the United States Permanent Representative to the United Nations. I have also served as Ambassador to Honduras (1981-1985), Mexico (1989-1993), the Philippines (1993-1996), and as Deputy Assistant to the President for National Security Affairs (1987-1989).

2. In the course of my official duties, I have been advised of this lawsuit and the allegations at issue in this case. The statements made herein are based on my personal knowledge, as well as on information provided to me in my official capacity as DNI, and on my

personal evaluation of that information. In personally considering this matter, I have executed a separate classified declaration dated June 30, 2006, and lodged *in camera* and *ex parte* in this case. Moreover, I have read and personally considered the information contained in the *In Camera, Ex Parte* Declaration of Lieutenant General Keith B. Alexander, Director of the National Security Agency, lodged in this case.

3. The purpose of this declaration is to formally assert, in my capacity as DNI and head of the United States Intelligence Community, the miliary and state secrets privilege (hereafter "state secrets privilege"), as well as a statutory privilege under the National Security Act, *see* 50 U.S.C. § 403-1(i)(1), in order to protect certain intelligence-related information implicated by the allegations in this case. Disclosure of the information covered by these privilege assertions would cause exceptionally grave damage to the national security of the United States and, therefore, should be excluded from any use in this case. In addition, I concur with General Alexander's conclusion that the risk is great that further litigation will lead to the disclosure of information harmful to the national security of the United States and, accordingly, this case should be dismissed.

THE DIRECTOR OF NATIONAL INTELLIGENCE

4. The position of Director of National Intelligence was created by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 1011(a) and 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of the Title I of the National Security Act of 1947). Subject to the authority, direction, and control of the President, the DNI serves as the head of the U.S. Intelligence Community and as the principal advisor to the President, the National Security Council, and the Homeland Security Council, for intelligence-related matters related to national security. *See* 50 U.S.C. § 403(b)(1), (2).

5. The "United States Intelligence Community" includes the Office of the Director

of National Intelligence; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the military services, the Federal Bureau of Investigation, the Department of Treasury, the Department of Energy, Drug Enforcement Administration, and the Coast Guard; the Bureau of Intelligence and Research of the Department of State; the elements of the Department of Homeland Security concerned with the analysis of intelligence information; and such other elements of any other department or agency as may be designated by the President, or jointly designated by the DNI and heads of the department or agency concerned, as an element of the Intelligence Community. *See* 50 U.S.C. § 401a(4).

6. The responsibilities and authorities of the DNI are set forth in the National Security Act, as amended. *See* 50 U.S.C. § 403-1. These responsibilities include ensuring that national intelligence is provided to the President, the heads of the departments and agencies of the Executive Branch, the Chairman of the Joint Chiefs of Staff and senior military commanders, and the Senate and House of Representatives and committees thereof. 50 U.S.C. § 403-1(a)(1). The DNI is also charged with establishing the objectives of, determining the requirements and priorities for, and managing and directing the tasking, collection, analysis, production, and dissemination of national intelligence by elements of the Intelligence Community. *Id.* § 403-1(f)(1)(A)(i) and (ii). The DNI is also responsible for developing and determining, based on proposals submitted by heads of agencies and departments within the Intelligence Community, an annual consolidated budget for the National Intelligence Program for presentation to the President, and for ensuring the effective execution of the annual budget for intelligence and intelligence-related activities, and for managing and allotting appropriations for the National

Intelligence Program. *Id.* § 403-1(c)(1)-(5).

7. In addition, the National Security Act of 1947, as amended, provides that "The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 403-1(i)(1). Consistent with this responsibility, the DNI establishes and implements guidelines for the Intelligence Community for the classification of information under applicable law, Executive Orders, or other Presidential directives and access and dissemination of intelligence. *Id.* § 403-1(i)(2)(A), (B). In particular, the DNI is responsible for the establishment of uniform standards and procedures for the grant of access to Sensitive Compartmented Information ("SCI") to any officer or employee of any agency or department of the United States, and for ensuring consistent implementation of those standards throughout such departments and agencies. *Id.* § 403-1(j)(1), (2).

8. By virtue of my position as the DNI, and unless otherwise directed by the President, I have access to all intelligence related to the national security that is collected by any department, agency, or other entity of the United States. Pursuant to Executive Order No. 12958, 3 C.F.R. § 333 (1995), as amended by Executive Order 13292 (March 25, 2003), reprinted as amended in 50 U.S.C.A. § 435 at 93 (Supp. 2004), the President has authorized me to exercise original TOP SECRET classification authority. My classified declaration, as well as the classified declaration of General Alexander on which I have relied in this case, are properly classified under § 1.3 of Executive Order 12958, as amended, because the public disclosure of the information contained in those declarations could reasonably be expected to cause exceptionally grave damage to national security of the United States.

ASSERTION OF THE STATE SECRETS PRIVILEGE

9. After careful and actual personal consideration of the matter, I have determined that the disclosure of certain information implicated by Plaintiffs' claims—as set forth here and

described in more detail in my classified declaration and in the classified declaration of General Alexander—would cause exceptionally grave damage to the national security of the United States and, therefore, such information must be protected from disclosure and excluded from this case. Accordingly, as to this information, I formally invoke and assert the state secrets privilege. In addition, it is my judgment that any attempt to proceed in the case will substantially risk the disclosure of the privileged information described briefly herein and in more detail in the classified declarations, and will cause exceptionally grave damage to the national security of the United States.

10. Through this declaration, I also invoke and assert a statutory privilege held by the DNI under the National Security Act to protect intelligence sources and methods implicated by this case. *See* 50 U.S.C. § 403-1(i)(1). My assertion of this statutory privilege for intelligence information and sources and methods is coextensive with my state secrets privilege assertion.

INFORMATION SUBJECT TO CLAIMS OF PRIVILEGE

11. My assertion of the state secrets and statutory privileges in this case includes any information tending to confirm or deny (a) alleged intelligence activities, such as the alleged collection by the NSA of records pertaining to a large number of telephone calls, (b) an alleged relationship between the NSA and AT&T (either in general or with respect to specific alleged intelligence activities), and (c) whether particular individuals or organizations have had records of their telephone calls disclosed to the NSA. My classified declaration describes in further detail the information over which I assert privilege.

12. As a matter of course, the United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets. The harm of revealing such information should be obvious. If the United States confirms that it is conducting a particular intelligence activity, that it is gathering information from a particular source, or that

it has gathered information on a particular person, such intelligence-gathering activities would be compromised and foreign adversaries such as al Qaeda and affiliated terrorist organizations could use such information to avoid detection. Even confirming that a certain intelligence activity or relationship does *not* exist, either in general or with respect to specific targets or channels, would cause harm to the national security because alerting our adversaries to channels or individuals that are not under surveillance could likewise help them avoid detection. In addition, denying false allegations is an untenable practice. If the government, for example, were to confirm in certain cases that specific intelligence activities, relationships, or targets do not exist, but then refuse to comment (as it would have to) in a case involving an actual intelligence activity, relationship, or target, a person could easily deduce by comparing such responses that the latter case involved an actual intelligence activity, relationship, or target. Any further elaboration on the public record concerning these matters would reveal information that would cause the very harms that my assertion of privilege is intended to prevent. The classified declaration of General Alexander that I considered in making this privilege assertion, as well as my own separate classified declaration, provide a more detailed explanation of the information at issue and the harms to national security that would result from its disclosure.

13. The information covered by my privilege assertion includes, but is not limited to, any such information necessary to respond to Plaintiffs' First Amended Complaint, Plaintiffs' Motion for a Preliminary Injunction, or Plaintiffs' First Set of Interrogatories.

CONCLUSION

14. In sum, I formally assert the state secrets privilege, as well as a statutory privilege under the National Security Act, 50 U.S.C. § 403-1(i)(1), to prevent the disclosure of the information described herein and in my classified declaration, as well as General Alexander's classified declaration. Moreover, because the very subject matter of this lawsuit concerns alleged intelligence activities, the litigation of this case directly risks the disclosure of privileged intelligence-related information. Accordingly, I join with General Alexander in respectfully requesting that the Court dismiss this case to stem the harms to the national security of the United States that will occur if such information is disclosed.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: 6/30/06

JOHN D. NEGROPONTE
Director of National Intelligence

U. S. Department of Justice

Civil Division

Assistant Attorney General *Washington, D.C. 20530*

July 28, 2006

VIA FACSIMILE AND FEDERAL EXPRESS

Chairman Kurt Adams
Commissioner Sharon M. Reishus
Maine Public Utilities Commission
242 State Street, State House Station 18
Augusta, Maine 04333

Re: Docket No. 2006-274; June 23, 2006, Procedural Order

Dear Chairman Adams and Commissioner Reishus:

I write in regard to the pending request for the Maine Public Utilities Commission ("MPUC") to open an investigation into whether Verizon is cooperating in Maine with the National Security Agency ("NSA") and with respect to the June 23, 2006, Procedural Order ("Procedural Order"), enclosed hereto. I understand that in considering whether to open an investigation the MPUC also is considering Verizon's motion to dismiss this proceeding. The United States appreciates the opportunity to provide its views to the MPUC. Please note, however, that our willingness to provide our views is not, and should not be deemed, either as a formal intervention in this matter or the submission of the United States to the jurisdiction of the State of Maine.

It is the position of the United States that the MPUC should decline to open an investigation of this matter and grant Verizon's motion to dismiss. To open an investigation would be a fruitless endeavor because the MPUC would be unable to obtain the information needed to reach a decision on the merits of the complaint. Any document request or other discovery propounded against Verizon in this proceeding would place Verizon in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without harming national security. Further, any effort by the MPUC to enforce compliance with such requests for information would be inconsistent with, and preempted by, federal law. Indeed, such requests for information would infringe upon federal operations, are contrary to federal law, and accordingly are invalid under the Supremacy Clause of the United States Constitution. Any such requests for information would seek disclosure of information regarding the Nation's foreign-intelligence gathering, but foreign-intelligence gathering is an exclusively federal

function. Responding to any such requests for information, including disclosing whether or to what extent any responsive materials exist, moreover, would violate various specific provisions of federal statutes and Executive Orders.

I note that the MPUC recognizes this problem insofar as the Procedural Order states the "more difficult issue is whether certain federal statutes and/or the so-called 'state secrets privilege' will prevent [the MPUC] from obtaining relevant information in the course of a Commission investigation." *See* Procedural Order at 2. I agree that resolving this issue "directly, in the correct forum" is an important consideration. Toward that end, this letter outlines the basic reasons why, in our view, any request for information in this proceeding would be preempted by federal law and that compliance with such requests would violate federal law. In similar situations in both New Jersey and Missouri, the United States has acted to protect its sovereign interests by filing lawsuits to preclude the enforcement of subpoenas that seek disclosure of similar information. We sincerely hope that, in light of governing law and the national security concerns implicated by the requests for information, you will decline to open an investigation and close these proceedings, thereby avoiding litigation over the matter. The United States very much appreciates your consideration of its position.

1. There can be no question that potential requests for information relevant to any investigation in this proceeding would interfere with and seek the disclosure of information regarding the Nation's foreign-intelligence gathering. But it has been clear since at least *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316 (1819), that state law may not regulate the Federal Government or obstruct federal operations. And foreign-intelligence gathering is an exclusively federal function; it concerns three overlapping areas that are peculiarly the province of the National Government: foreign relations and the conduct of the Nation's foreign affairs, *see American Insurance Ass'n v. Garamendi*, 539 U.S. 396, 413 (2003); the conduct of military affairs, *see Sale v. Haitian Centers Council*, 509 U.S. 155, 188 (1993) (President has "unique responsibility" for the conduct of "foreign and military affairs"); and the national security function. As the Supreme Court of the United States has stressed, there is "paramount federal authority in safeguarding national security," *Murphy v. Waterfront Comm'n of New York Harbor*, 378 U.S. 52, 76 n.16 (1964), as "[f]ew interests can be more compelling than a nation's need to ensure its own security." *Wayte v. United States*, 470 U.S. 598, 611 (1985).

To illustrate that Verizon could not comply with such requests for information without harming national security, I direct your attention to the now withdrawn requests of the lead complainant.[1] The requests for information demand that Verizon produce information regarding alleged interception of communications by the NSA as well as a purported contract with the NSA

[1] Although the lead complainant withdrew these requests, he also states that he "*will refile them*, should the Commission decide to open an investigation in this case." *See* Letter of May 17, 2006, from Lead Complainant to Dennis Keschl at 1 (emphasis added).

to allegedly provide customer records to the NSA. *See* Complainant's 1st Data Request to Verizon of May 9, 2006 (incorporating January 20, 2006 requests from Representative Conners) & Complainant's 2d Data Request to Verizon of May 15, 2006. Thus, the requests seek information, including *inter alia*: whether Verizon has "ever given the government access to any . . . hardware or software used to deliver communications servies in response to a request that was not compelled" by certain designated processes; whether Verizon "ever turned over customer records to the federal government in response to a request that was not compelled" by certain designated processes; "how many call records in total has Verizon provided to NSA;" "how many are its Maine customers' records , and how many of those are records of those customers' intrastate calls;" and "[b]y what processes does Verizon provide NSA its customers' call records." *See id.* Should the MPUC open an investigation and complainants refile these requests, or if the MPUC itself seeks its own similar discovery, such an exertion of regulatory authority[2] with respect to the nation's foreign-intelligence gathering would seek to use state regulatory authority to intrude upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with federal prerogatives. That effort is fundamentally inconsistent with the Supremacy Clause. *McCulloch*, 17 U.S. at 326-27 (1819) ("[T]he states have no power . . . to retard, impede, burden, or in any manner control, the operations of the constitutional laws enacted by Congress to carry into execution the power vested in the general government."); *see also Leslie Miller, Inc. v. Arkansas*, 352 U.S. 187 (1956).

The Supreme Court's decision in *American Insurance Ass'n v. Garamendi*, 539 U.S. 396 (2003), is the most recent precedent that demonstrates that such state-law based information requests are preempted by federal law. In *Garamendi*, the Supreme Court held invalid subpoenas issued by the State of California to insurance carriers pursuant to a California statute that required those carriers to disclose all policies sold in Europe between 1920 and 1945, concluding that California's effort to impose such disclosure obligations interfered with the President's conduct of foreign affairs. Here, such requests for information would seek the disclosure of information that infringes on the Federal Government's intelligence gathering authority and on the Federal Government's role in protecting the national security at a time when we face terrorist threats to the United States homeland; any such requests for information, just like the subpoenas at issue in *Garmendi*, are preempted. Under the Supremacy Clause, "a state may not interfere with federal action taken pursuant to the exclusive power granted under the United States Constitution or under congressional legislation occupying the field." *Abraham v. Hodges*, 255 F. Supp. 2d 539, 549 (D.S.C. 2002) (enjoining the state of South Carolina from interfering with the shipment of nuclear waste, a matter involving the national security, because "when the federal government acts within its own sphere or pursuant to the authority of Congress in a given field, a state may not interfere by means of conflicting attempt to promote its own local interests").

---

[2] Any such information request would likely fall under MPUC Rules of Procedure 821 or 822 regarding data requests or Rules of Procedure 730 and 731 regarding subpoena practice.

2. Responding to such requests for information, including merely disclosing whether or to what extent any responsive materials exist, would also violate various federal statutes and Executive Orders. Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note, provides: "[N]othing in this Act *or any other law* . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of persons employed by such agency."[3] *Ibid.* (emphasis added). Similarly, 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 ("DNI") the authority and responsibility to "protect intelligence sources and methods from unauthorized disclosure." *Ibid.*[4] (As set forth below, the DNI has determined that disclosure of the types of information sought by the information requests would harm national security.)

Several Executive Orders promulgated pursuant to the foregoing constitutional and statutory authority govern access to and handling of national security information. Of particular importance here, 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 comprehensive system for classifying, safeguarding, and declassifying national security information. It provides that a person may have access to classified information only where "a favorable determination of eligibility for access has been made by an agency head or the agency head's designee"; "the person has signed an approved nondisclosure agreement"; and "the person

---

[3] Section 6 reflects a "congressional judgment that in order to preserve national security, information elucidating the subjects specified ought to be safe from forced exposure." *The Founding Church of Scientology of Washington, D.C., Inc. v. Nat'l Security Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979); *accord Hayden v. Nat'l Security Agency*, 608 F.2d 1381, 1389 (D.C. Cir. 1979). Thus, in enacting Section 6, Congress was "fully aware of the 'unique and sensitive' activities of the [NSA] which require 'extreme security measures,'" *Hayden*, 608 F.2d at 1390 (citing legislative history), and "[t]he protection afforded by section 6 is, by its very terms, absolute. If a document is covered by section 6, NSA is entitled to withhold it. . . ." *Linder v. Nat'l Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996).

[4] The authority to protect intelligence sources and methods from disclosure is rooted in the "practical necessities of modern intelligence gathering," *Fitzgibbon v. CIA*, 911 F.2d 755, 761 (D.C. Cir. 1990), and has been described by the Supreme Court as both "sweeping," *CIA* v. *Sims*, 471 U.S. 159, 169 (1985), and "wideranging." *Snepp v. United States*, 444 U.S. 507, 509 (1980). Sources and methods constitute "the heart of all intelligence operations," *Sims*, 471 U.S. at 167, and "[i]t is the responsibility of the [intelligence community] to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the . . . intelligence-gathering process." *Id.* at 180.

has a need-to-know the information." That Executive Order further states 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). Exec. Order No. 13292, Sec. 4.1(a).

Finally, it is a federal crime to divulge to an unauthorized person specified categories of classified information, including information "concerning the communication intelligence activities of the United States." 18 U.S.C. § 798(a). The term "classified information" means "information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution," while an "unauthorized person" is "any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States." 18 U.S.C. § 798(b).

Neither Maine state officials nor the complainants have been authorized to receive classified information concerning the foreign-intelligence activities of the United States in accordance with the terms of the foregoing statutes or Executive Orders (or any other lawful authority). To the extent any MPUC (or complainant) request of information seeks to compel disclosure of such information to state officials or private parties, responding to them would obviously violate federal law.

3. The complainants' withdrawn data requests seek information on two alleged government programs that media reports claim involve the purported interception of communications and purported release of call records. In ongoing litigation in the United States District Courts for the Northern District of California and the Northern District of Illinois, the DNI has formally asserted the state secrets privilege regarding the very same topics and types of information sought by such requests for information. *See Hepting v. AT&T Corp.*, No. 06-0672-VRW (N.D. Cal.); *Terkel v. AT&T Corp.*, 06-cv-2837 (N.D. Il.). In *Terkel*, for example, Director Negroponte concluded with regard to the alleged records program that "the United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets" and that "[t]he harm of revealing such information should be obvious" because "[i]f the United States confirms that it is conducting a particular intelligence activity, that it is gathering information from a particular source, or that it has gathered information on a particular person, such intelligence-gathering activities would be compromised and foreign adversaries such as al Qaeda and affiliated terrorist organizations could use such information to avoid detection." *See* Unclassified Declaration of John D. Negroponte in *Terkel* ("Negroponte Decl.") ¶ 12, enclosed hereto. Furthermore, "[e]ven confirming that a certain intelligence activity or relationship does *not* exist, either in general or with respect to specific targets or channels, would cause harm to the national security because alerting our adversaries to channels or individuals that are not under surveillance could likewise help them avoid detection." *Id.*

Similar privilege assertions were made in *Hepting*. These concerns are particularly acute when we are facing the threat of terrorist attacks on United States soil.

In the recent *Terkel* decision, Judge Kennelly granted the Government's motion to dismiss the action, thereby upholding the DNI's assertion of the state secrets privilege. Having been "persuaded that requiring AT&T to confirm or deny whether it has disclosed large quantities of telephone records to the federal government could give adversaries of this country valuable insight into the government's intelligence activities, "the Court held that" such disclosures are barred by the state secrets privilege." *Terkel*, Slip. Op. at 32, enclosed hereto. In seeking to have telecommunication carriers confirm or deny similar information, the requests at issue here thus seek the very type of disclosures deemed inimical to the national security in *Terkel* by both the DNI and Judge Kennelly.[5]

In seeking information bearing upon NSA's purported involvement with various telecommunications carriers, any such requests for information would thus seek the disclosure of matters with respect to which the DNI already has determined that disclosure, including confirming or denying whether or to what extent such materials exist, would improperly reveal intelligence sources and methods. Accordingly, the state law upon which such requests for information would be based is inconsistent with and preempted by federal law as regards intelligence gathering, and also conflicts with the assertion of the state secrets privilege by the DNI. Any application of state law that would compel such disclosures notwithstanding the DNI's assessment would contravene the DNI's authority and the Act of Congress conferring that authority. More broadly, such requests for information would involve an improper effort to use state law to regulate or oversee federal functions, and would implicate significant issues under the Supremacy Clause.

* * *

---

[5] Although Judge Walker did not grant the government's motion to dismiss on state secrets grounds at this stage in *Hepting*, he declined to permit discovery on communications records allegations. The United States respectfully disagrees with his decision not to dismiss the case on state secrets ground; Judge Walker himself certified his order for immediate appeal, and the United States will appeal. In any event, however, a *federal court's* authority regarding the assertion of state secrets in no way whatsoever provides authority for a state administrative body, otherwise without authority under the Constitution in this area, to order the release of classified information or otherwise interfere with alleged federal government operations. With respect to the complainants' suggestion that the MPUC appoint an "expert" regarding classified information, *see* Letter of July 21, 2006, from Lead Complainant to Dennis Keschl, the MPUC has no greater authority to order the release of such information to an expert than it does to order the release of such information to itself.

Accordingly, for the reasons outlined above, it is the United States' position that any similar requests for information of the kind at issue in *Hepting* and *Terkel* that are relevant to the proposed investigation are inconsistent with and preempted under the Supremacy Clause, and that compliance with such requests would place Verizon in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without causing harm to the national security. For these reasons, we urge you to decline to open an investigation and to close these proceedings, as the MPUC will be unable to obtain the information it needs consider the complaint and so that litigation over this matter may be avoided.

Please do not hesitate to contact me if you have any questions. As noted, your consideration of this matter is very much appreciated.

Sincerely,

Peter D. Keisler
Assistant Attorney General

Enclosures

cc: ME Docket 2006-274 service list

STATE OF MAINE
PUBLIC UTILITIES COMMISSION

Docket No. 2006-274

August 9, 2006

MAINE PUBLIC UTILITIES COMMISSION
Request for Commission Investigation into Whether Verizon is Cooperating in Maine With the National Security Agency's Warrantless Domestic Wiretapping Program

ORDER

ADAMS, Chairman; REISHUS, Commissioner

I. SUMMARY

In this order we require that Verizon provide sworn affirmations of representations it made in its filed response to the complaint in this matter.

II. BACKGROUND

James D. Cowie, on behalf of himself and 21 other persons, has filed a complaint, pursuant to 35-A M.R.S.A. § 1302(1), requesting that the Commission investigate whether and to what extent Verizon has cooperated with the National Security Agency (NSA) in connection with two alleged intelligence gathering programs. Specifically, the petitioners ask the Commission to determine "whether Verizon has provided the NSA, or any other government agency, unwarranted access to any Verizon or MCI facilities in Maine, or to records of domestic or international calls or e-mails made or received by their customers in Maine." In the event that we find that Verizon has so cooperated, petitioners also seek an order enjoining further cooperation.

For its factual basis, the complaint cites a series of reports published late last year by the New York Times and the Los Angeles Times asserting that another telecommunications company, AT&T, had installed in its switching machines a circuit designed by the NSA to provide access to phone calls and/or records of phone calls. These articles report, further, that AT&T maintains a database which keeps track of phone numbers on both ends of calls and that the NSA was able to interface directly with the database. The implication, drawn by the articles, is that with the cooperation of telecommunications firms the NSA is conducting a call data program ("data mining program") in which it uses statistical methods to analyze patterns in the calling activity of vast numbers of users. Relying on these articles, the complainants ask us to determine not only whether Verizon provided to the federal government records of customer telephone calls or e-mail communications, but also whether it granted access to the telecommunications facilities and infrastructure of Verizon or MCI, located in Maine, such that the NSA (or any other federal agency) could, thereafter, obtain call records and e-mail records directly, and on its own initiative.

The articles upon which the complainants rely also report that the NSA has been eavesdropping on Americans and others inside the United States in order to search for evidence of terrorist activity, and that it is doing so with authorization from the President

but without first obtaining warrants that are typically required for domestic spying. The complainants therefore also seek an investigation into the extent of Verizon's cooperation, in Maine, with this eavesdropping program.

Verizon, in its response to the complaint, contends that it can neither admit nor deny involvement in national security matters and that an investigation into this matter would be fruitless because we will be unable to ascertain facts germane to the central allegations of the complaint. The United States Department of Justice (DOJ), which filed comments at our request, supports Verizon's contention.

Notwithstanding its claimed inability to discuss its relationship to any classified NSA programs, Verizon's written response to the complaint, filed on May 19, 2006, includes several affirmative assertions of fact in support of its argument that we should decline to open an investigation. Specifically, Verizon's filed response refers to two press releases, issued on May 12, 2006 and May 16, 2006, copies of which are appended as exhibits to the filing. These press releases make the following representations:

1. Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records from any of its businesses, or any call data from those records.

2. None of these companies – wireless or wireline – provided customer records or call data.

3. Verizon's wireless and wireline companies did not provide to NSA customer records or call data, local or otherwise.

4. Verizon will provide customer information to a government agency only where authorized by law for appropriately-defined and focused purposes.

5. When information is provided, Verizon seeks to ensure it is properly used for that purpose and is subject to appropriate safeguards against improper use.

6. Verizon does not, and will not, provide any government agency unfettered access to its customer records or provide information to the government under circumstances that would allow a fishing expedition.

7. Verizon acquired MCI, and Verizon is ensuring that Verizon's policies are implemented at that entity and that all its activities fully comply with law.

These seven representations were made to the Commission for the purpose of influencing the Commission's decision as to whether or not to open an investigation. Maine law provides that statements made in any document filed with the Commission must be truthful. Specifically, 35-A M.R.S.A. § 1507-A makes it a crime for "any person to

make or cause to be made, in any document filed with the commission or in any proceeding under this Title, any statement that, at the time and in light of the circumstances under which it is made, is false in any material respect and that the person knows is false in any material respect."

III. DISCUSSION AND DECISION

The Maine Public Utilities Commission serves the people of Maine, and has an important role in providing a forum for grievances by citizens of this state against utilities that serve them. Moreover, Maine telecommunications subscribers have a right to the privacy of their communications over our telephone system, as well as over the dissemination of their telephone records, including their telephone numbers. We must open an investigation into the allegations that Verizon's activities violate its customers' privacy rights unless we find that Verizon has taken adequate steps to remove the cause of the complaint or that the complaint is without merit. 35-A M.R.S.A. § 1302(2).

If the seven representations identified above are in fact true, such statements could satisfy the concerns raised in the complaint. To be plain, we read Verizon's representations as denying that it provided customer records or call data associated with its customers in Maine to agencies of the federal government, and that it did not provide such agencies with access to its facilities or infrastructure in Maine such that those agencies would have direct, unfettered access to Verizon's network or the data it carries.

However, we are unwilling to rely on these representations to dismiss the complaint because they do not bear sufficient indicia of truth as they are not attributed to an individual within Verizon who has decision-making authority and knowledge of the matters asserted. As noted above, we may only dismiss the complaint if we find that Verizon has taken adequate steps to remove the cause of the complaint or if the complaint lacks merit. 35-A M.R.S.A. § 1302(2).

In order to fulfill our duty to consider whether to open an investigation as set forth in 35-A M.R.S.A. § 1302, we find that we require as to each of the seven representations set forth above a sworn affirmation that such representation is true and not misleading in light of the circumstances in which it is made. Pursuant to our authority set forth in 35-A M.R.S.A. § 112(2), we therefore order that Verizon obtain such affirmations made under oath by an officer of Verizon with decision-making authority and knowledge covering the subject matters asserted therein. Verizon shall file these affirmations on or before August 21, 2006.

Pending our receipt of the affirmations from Verizon, we neither open an investigation nor dismiss the complaint. To the parties, and to the Office of the Public Advocate, the Maine Civil Liberties Union, Christopher Branson, Esq., and the Department of Justice, we note our appreciation of the well reasoned and articulate comments that have been filed in this matter.

IV. CONCLUSION

For the foregoing reasons, we order that Verizon file, on or before August 21, 2006, an affirmation that each of the seven (7) enumerated representations identified in Section II is both true and not misleading in light of the circumstances in which such affirmation is provided, and that such affirmation be made under oath by an officer of Verizon with decision-making authority and knowledge covering the subject matters asserted therein.

Dated at Augusta, Maine, this 9th day of August, 2006.

BY ORDER OF THE COMMISSION

_____

Dennis L. Keschl
Acting Administrative Director

COMMISSIONERS VOTING FOR: Adams
Reishus