



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

Exhibit 1
Page 1 of 3

May 22, 2006

The Honorable Edward J. Markey
Ranking Member
Subcommittee on Telecommunications and the Internet
Energy and Commerce Committee
U.S. House of Representatives
2108 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressman Markey:

Thank you for your letter regarding recent media reports concerning the collection of telephone records by the National Security Agency. In your letter, you note that section 222 of the Communications Act provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers." 47 U.S.C. § 222(a). You have asked me to explain the Commission's plan "for investigating and resolving these alleged violations of consumer privacy."

I know that all of the members of this Commission take very seriously our charge to faithfully implement the nation's laws, including our authority to investigate potential violations of the Communications Act. In this case, however, the classified nature of the NSA's activities makes us unable to investigate the alleged violations discussed in your letter at this time.

The activities mentioned in your letter are currently the subject of an action filed in the United States District Court for the Northern District of California. The plaintiffs in that case allege that the NSA has "arrang[ed] with some of the nation's largest telecommunications companies . . . to gain direct access to . . . those companies' records pertaining to the communications they transmit." *Hepting v. AT&T Corp.*, No. C-06-0672-VRW (N.D. Cal.), Amended Complaint ¶ 41 (Feb. 22, 2006). According to the complaint, for example, AT&T Corp. has provided the government "with direct access to the contents" of databases containing "personally identifiable customary proprietary network information (CPNI)," including "records of nearly every telephone communication carried over its domestic network since approximately 2001, records that include the originating and terminating telephone numbers and the time and length for each call." *Id.* ¶¶ 55, 56, 61; *see also, e.g.*, Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today* A1 (May 11, 2006) (alleging that the NSA "has been secretly collecting the phone call records of tens of millions of Americans, using data provided" by major telecommunications carriers).

The government has moved to dismiss the action on the basis of the military and state secrets privilege. *See Hepting*, Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America (May 12, 2006). Its motion is accompanied by declarations from John D. Negroponte, Director of National Intelligence, and Lieutenant General Keith B. Alexander, Director, National Security Agency, who have maintained that disclosure of information “implicated by Plaintiffs’ claims . . . could reasonably be expected to cause exceptionally grave damage to the national security of the United States.” Negroponte Decl. ¶ 9. They specifically address “the NSA’s purported involvement” with specific telephone companies, noting that “the United States can neither confirm nor deny alleged NSA activities, relationships, or targets,” because “[t]o do otherwise when challenged in litigation would result in the exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general.” Alexander Decl. ¶ 8.

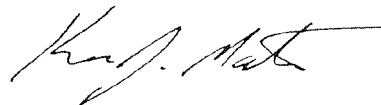
The representations of Director Negroponte and General Alexander make clear that it would not be possible for us to investigate the activities addressed in your letter without examining highly sensitive classified information. The Commission has no power to order the production of classified information. Rather, the Supreme Court has held that “the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it. Certainly, it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment.” *Department of the Navy v. Egan*, 484 U.S. 518, 529 (1988).

The statutory privilege applicable to NSA activities also effectively prohibits any investigation by the Commission. The National Security Act of 1959 provides that “nothing 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] of any information with respect to the activities thereof.” Pub. L. No. 86-36, § 6(a), 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note. As the United States Court of Appeals for the District of Columbia Circuit has explained, the statute’s “explicit reference to ‘any other law’ . . . must be construed to prohibit the disclosure of information relating to NSA’s functions and activities as well as its personnel.” *Linder v. NSA*, 94 F.3d 693, 696 (D.C. Cir. 1996); *see also Hayden v. NSA/Central Sec. Serv.*, 608 F.2d 1381, 1390 (D.C. Cir. 1979) (“Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful.”). This statute displaces any authority that the Commission might otherwise have to compel, at this time, the production of information relating to the activities discussed in your letter.

Page 3—The Honorable Edward J. Markey

I appreciate your interest in this important matter. Please do not hesitate to contact me if you have further questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Kevin J. Martin". The signature is fluid and cursive, with a long horizontal stroke extending from the end.

Kevin J. Martin
Chairman



COMMONWEALTH OF PENNSYLVANIA
PENNSYLVANIA PUBLIC UTILITY COMMISSION
P.O. BOX 3265, HARRISBURG, PA 17105-3265

Exhibit 2
Page 1 of 21

ISSUED: August 18, 2006

IN REPLY PLEASE
REFER TO OUR FILE
C-20066397 et al

SUZAN DEBUSK PAIVA ESQUIRE
VERIZON PENNSYLVANIA INC
1717 ARCH STREET 32N
PHILADELPHIA PA 19103

ACLU of Pennsylvania, et al.
V.
AT&T Communications of PA, LLC, et al.

TO WHOM IT MAY CONCERN:

Enclosed is a copy of the Initial Decision of Administrative Law Judge Charles E. Rainey, Jr. This decision is being issued and mailed to all parties on the above specified date.

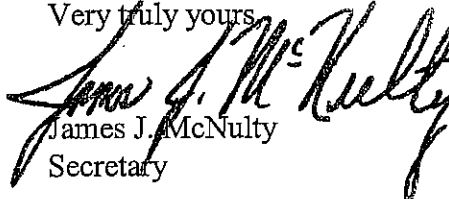
If you do not agree with any part of this decision, you may send written comments (called Exceptions) to the Commission. Specifically, an original and nine (9) copies of your signed exceptions MUST BE FILED WITH THE SECRETARY OF THE COMMISSION 2ND FLOOR KEYSTONE BUILDING, NORTH STREET, HARRISBURG, PA OR MAILED TO P.O. BOX 3265, HARRISBURG, PA 17105-3265, within twenty (20) days of the issuance date of this letter. The signed exceptions will be deemed filed on the date actually received by the Secretary of the Commission or on the date deposited in the mail as shown on U.S. Postal Service Form 3817 certificate of mailing attached to the cover of the original document (52 Pa. Code §1.11(a)) or on the date deposited with an overnight express package delivery service (52 Pa. Code 1.11(a)(2), (b)). If your exceptions are sent by mail, please use the address shown at the top of this letter. A copy of your exceptions must also be served on each party of record. 52 Pa. Code §1.56(b) cannot be used to extend the prescribed period for the filing of exceptions/reply exceptions. A certificate of service shall be attached to the filed exceptions.

If you receive exceptions from other parties, you may submit written replies to those exceptions in the manner described above within ten (10) days of the date that the exceptions are due.

Exceptions and reply exceptions shall obey 52 Pa. Code 5.533 and 5.535 particularly the 40-page limit for exceptions and the 25-page limit for replies to exceptions. Exceptions should clearly be labeled as "EXCEPTIONS OF (name of party) - (protestant, complainant, staff, etc.)".

If no exceptions are received within twenty (20) days, the decision of the Administrative Law Judge may become final without further Commission action. You will receive written notification if this occurs.

Very truly yours,


James J. McNulty
Secretary

Encls.
Certified Mail
Receipt Requested
jeh

RECEIVED AUG 22 2006

**BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION**

ACLU of Pennsylvania, et al.	:	
v.	:	C-20066397
AT&T Communications of PA LLC	:	
ACLU of Pennsylvania, et al.	:	
v.	:	C-20066398
Verizon Pennsylvania Inc.	:	
ACLU of Pennsylvania, et al.	:	
v.	:	C-20066399
Verizon North Incorporated	:	
ACLU of Pennsylvania, et al.	:	
v.	:	C-20066401
CTSI, LLC	:	
ACLU of Pennsylvania, et al.	:	
v.	:	C-20066404
ARC Networks Inc.	:	
CWA District 13/Terrance T. Tipping	:	
v.	:	C-20066410
Verizon Pennsylvania Inc.	:	
CWA District 13/Terrance T. Tipping	:	
v.	:	C-20066411
Verizon North Incorporated	:	

CWA District 13/Terrance T. Tipping

v.

Verizon Select Services Inc.

C-20066412

CWA District 13/Terrance T. Tipping

v.

AT&T Communications of PA LLC

C-20066413

INITIAL DECISION

Before
Charles E. Rainey, Jr.
Administrative Law Judge

HISTORY OF THE PROCEEDING

I. ACLU Complaints

On May 24, 2006, American Civil Liberties Union of Pennsylvania, Pennsylvania Coalition Against Domestic Violence, HAVIN, Inc., William Way Community Center, AIDS Community Alliance of South Central PA, Common Roads, Alyce Bowers, Katherine Franco, Lynne French, Louis M. Gehosky, David M. Jacobson, Rev. Robin Jarrell, Stephanie Parke, Marie Poulsen, Gregory Stewart, Barbara Sutherland, Francis Walsh, Michael Wolf and John Wolff (collectively referred to herein as "ACLU") filed a formal complaint against AT&T Communications of Pennsylvania (AT&T), Verizon Pennsylvania Inc. and Verizon North Inc. (collectively referred to herein as "Verizon"), CTSI, LLC (CTSI) and ARC Networks Inc. d/b/a InfoHighway Communications (InfoHighway)¹ with the Pennsylvania Public Utility

¹ ACLU's complaint was also filed against United Telephone Company of Pennsylvania d/b/a Embarq Pennsylvania (C-20066400), Denver & Ephrata Telephone & Telegraph Company (C-20066402) and Buffalo Valley Telephone Company (C-20066403). However, by letters filed July 12, 2006, ACLU withdrew the complaint against Denver & Ephrata Telephone Company and Buffalo Valley Telephone Company. And by letter filed July 17, 2006, ACLU withdrew the complaint against United Telephone Company of Pennsylvania. The Commission treated the letters as petitions for leave to withdraw the complaint as to those respondents, and when no timely objections were filed, the Commission closed the cases as to those respondents.

Commission (Commission) pursuant to 52 Pa. Code §§5.21 (Formal complaints generally) and 63.135 (Customer information)². ACLU alleges that it believes that respondents violated 52 Pa. Code §63.135 by voluntarily disclosing to the National Security Agency (NSA) (without requiring the production of a search warrant or court order), the personal calling patterns of millions of Pennsylvania telephone customers, including telephone numbers called, and the time, date and direction of calls. The Commission's Secretary's Bureau divided the complaint into separate complaints against each of the named telecommunications carriers, and assigned each complaint a separate docket number. The Commission's Secretary's Bureau then served a copy of the complaint on each of the named respondents. See, 66 Pa.C.S. §702 (Service of complaints on parties).

On June 20, 2006, AT&T filed an answer and preliminary objection in the nature of a motion to dismiss the complaint at docket number C-20066397. On June 21, 2006, AT&T filed an affidavit as a supplement to its answer.

On June 20, 2006, Verizon filed in regard to the complaints at docket numbers C-20066398 and C-20066399, preliminary objections and a "response".

On June 20, 2006, CTSI filed at docket number C-20066401 an answer and "new matter directed to complainants" and "new matter directed to co-respondents".

Filed at docket number C-20066404 on June 21, 2006, is a letter in lieu of an answer, authored by Jeffrey E. Ginsberg, the Chairman of InfoHighway.

On June 26, 2006, ACLU filed a letter requesting a 10-day extension of time to file responses to the motions of AT&T and Verizon.³ On June 26, 2006, ACLU filed a letter stating that AT&T had no objection to its request. By Notice dated June 27, 2006, the parties

² In the complaint, ACLU actually refers to these Sections as being under the Public Utility Code. However, they are not. The Public Utility Code provides the Commission's statutory authority, and those statutes are found under Title 66 of the Pennsylvania Consolidated Statutes. The Sections referenced by ACLU are Commission regulations found under Title 52 of the Pennsylvania Code.

³ ACLU's letter also requested an extension of time to respond to preliminary objections filed by Denver & Ephrata Telephone & Telegraph Company and Buffalo Valley Telephone Company. However, as previously noted, ACLU subsequently withdrew its complaint as to those companies.

were informed that ACLU's request for an extension of time was granted and that the motions were required to be filed on or before July 17, 2006. On July 14, 2006, ACLU filed responses to the motions.

On August 2, 2006, AT&T filed a "Supplement" to its motion to dismiss the complaint at docket number C-20066397.

II. CWA Complaints

On May 24, 2006, District 13 of the Communications Workers of America and its Assistant to the Vice President, Terrance T. Tipping, (collectively referred to herein as "CWA") filed formal complaints against Verizon (including Verizon Pennsylvania Inc., Verizon North Inc. and Verizon Select Services Inc.) (C-20066410, C-20066411 and C-20066412) and AT&T (C-20066413). CWA alleges that Verizon and AT&T possibly engaged in "unreasonable utility practices" if they participated in "the NSA's domestic wiretapping program." The Commission's Secretary's Bureau served copies of the complaints on the appropriate respondents.

On June 20, 2006, Verizon filed in regard to the complaints at docket numbers C-20066410, C-20066411 and C-20066412, preliminary objections and a "response".

Also on June 20, 2006, Verizon filed at the aforementioned docket numbers, a motion for the admission *pro hac vice* of Leigh A. Hyer, Esquire. No timely objections to the motion for admission *pro hac vice* were filed. Verizon's motion for the admission *pro hac vice* of Leigh A. Hyer, Esquire is granted.

On June 22, 2006, AT&T filed an answer and preliminary objection in the nature of a motion to dismiss CWA's complaint at docket number C-20066413.

CWA did not file a timely answer or response to either the preliminary objections of Verizon or the preliminary objection in the nature of a motion to dismiss of AT&T. I also note that CWA did not file a request for an extension of time to file an answer or response.

III. Consolidation of complaints

Commission rules provide in pertinent part:

§5.81 Consolidation.

(a) The Commission or presiding officer, with or without motion, may order proceedings involving a common question of law or fact to be consolidated. The Commission or presiding officer may make orders concerning the conduct of the proceeding as may avoid unnecessary costs or delay.

52 Pa. Code §5.81(a). The ACLU and CWA complaints involve common questions of law and fact. I am therefore consolidating the ACLU and CWA complaints for the purpose of adjudicating this matter.

DISCUSSION

The basis of ACLU's complaint is principally an article that appeared in *USA Today* on May 11, 2006, as well as articles that appeared shortly thereafter in the *New York Times* and *Wall Street Journal*. Complaint at 8-10, 12. Based on those articles, ACLU alleges that it believes that since September 11, 2001, AT&T and Verizon violated 52 Pa. Code §63.135 by voluntarily disclosing to the NSA, (and not requiring it to produce a search warrant or court order), the personal calling patterns of millions of Pennsylvania customers, including telephone numbers called, time, date and direction of calls. *Id.* at 2, 9, 13. ACLU also alleges that it "reasonably believe[s]" that the other respondents named in its complaint have and are committing the same violation. *Id.* at 13. ACLU further alleges that with the information provided by respondents, the NSA "can easily determine the names and addresses associated with these calls by cross-referencing other readily available databases." *Id.* at 2, 9. ACLU requests that the Commission order respondents to: (1) provide ACLU and the Commission with a complete accounting of any and all releases of customer information to the NSA or any other

federal or state law enforcement agency⁴ that was not compelled by court order or warrant to cease and desist from releasing customer calling information to the NSA or other law enforcement agencies without court order or warrant; and (3) take such steps as are necessary to comply with Pennsylvania law. *Id.* at 14. ACLU also seeks “such other relief as the Commission may deem necessary and proper.” *Id.* at 14.

CWA indicates that its complaints are based on “official statements and press releases” regarding “the NSA’s domestic wiretapping program.” CWA alleges that Verizon and AT&T possibly engaged in “unreasonable utility practices” if they participated in the NSA’s domestic wiretapping program. CWA requests that the Commission investigate whether respondents are “cooperating in Pennsylvania, with the National Security Agency’s (NSA) warrantless domestic wiretapping program.” Specifically, CWA requests that the Commission “use its statutory authority” to compel respondents to answer four questions. Those four questions are:

1. [Have respondents] provided NSA with unwarranted access to call records, e-mail records and unwarranted access to [respondents’] facilities in Pennsylvania?⁵
2. [Have respondents] allowed the NSA to tap calls and read e-mails of [respondents’] customers in Pennsylvania?
3. [Have respondents] provided data mining samples of telephone calls and e-mails to NSA?
4. [Have respondents] allowed telephone and e-mail data to be directly sampled by NSA?

See, attachments to CWA’s completed formal complaint forms.

In its preliminary objection in the nature of a motion to dismiss the complaints of ACLU and CWA, AT&T argues that the Commission lacks jurisdiction to hear the complaints.

⁴ My references in this Initial Decision to “the NSA” includes any other law enforcement and governmental agencies which complainants allege may have received customer calling information from respondents.

⁵ The question marks after the questions were supplied. In the attachments to the complaints, the questions were punctuated with periods.

AT&T asserts that at the core of complainants' complaints are significant legal issues governed exclusively by federal law which divests the states of any power to act. AT&T Motion at 1-2. Those significant legal issues according to AT&T are: (1) the scope of authority of the Executive Branch of the United States government to conduct intelligence-gathering activities in furtherance of national security; and (2) the ability of the United States to protect classified information. Id. at 1.

AT&T asserts that at least two federal statutes, 18 U.S.C. §798 and 50 U.S.C. §402 (§6 of the National Security Agency Act of 1959), preempt proceedings before the Commission on the complaints. Id. at 10. AT&T notes that 18 U.S.C. §798 makes it a felony to "knowingly and willfully communicate, furnish, transmit, or otherwise make available to an unauthorized person, or publish, or use in any manner prejudicial to the safety or interest of the United States,...any classified information...concerning the communication intelligence activities of the United States." Id. at 11. And AT&T notes that §6 of the National Security Agency Act ("the Act") prohibits the disclosure of any information regarding the activities of the NSA. Id. at 12. Specifically, the Act provides that "nothing 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." 50 U.S.C. §402. Id. at 12.

AT&T emphasizes that "[t]he United States has repeatedly emphasized that the NSA program and all of its operational details, including the existence or non-existence of participation by particular telecommunication carriers, is highly classified." Id. at 11. AT&T avers that the United States Department of Justice sent it a letter dated June 14, 2006, warning it that "responding to subpoenas [issued by the New Jersey Attorney General] – including by disclosing whether or to what extent any responsive materials exist – would violate federal laws and Executive Orders." Id. at 8. AT&T argues that therefore it would violate federal criminal statutes if it participated in any state investigation, as it would be required, at a minimum, to disclose whether it was in possession of relevant information. Id. at 12.

AT&T points out that the Federal Communications Commission (FCC) declined to undertake an investigation after it determined that any investigation would require the

production of classified information relating to NSA activities, and that it, the FCC, lacks the authority to compel the production of classified information. Id. at 13. AT&T opines that the Commission should make the same determination in regard to the present complaints. Id.

AT&T argues that a Commission investigation into the complaints of ACLU and CWA is also barred by the state secrets privilege, the Totten rule, the Communication Assistance to Law Enforcement Act (CALEA) and the Foreign Intelligence Act (FISA). Citing Ellsberg v. Mitchell, 709 F.2d 51, 57 (D.C. Cir. 1983), AT&T explains that “[t]he state secrets privilege is a constitutionally-based privilege belonging exclusively to the federal government that protects any information whose disclosure would result in impairment of the nation’s defense capabilities.” AT&T Motion at 14. The Totten rule, according to AT&T, provides that “the existence of a contract for secret services with the government is itself a fact not to be disclosed.” Totten v. United States, 92 U.S. 105, 107 (1875). Id. at 17. And AT&T states that CALEA, 47 U.S.C. §1001 et seq., provides at §1002(a) that, with certain exceptions, “a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of, among other things, expeditiously isolating and enabling the government to intercept wire and electronic communications of a particular subscriber and expeditiously isolating and enabling the government...to access call-identifying information that is reasonably available to the carrier.” Id. at 19. AT&T also explains that FISA “authorizes the federal government to obtain an order directing telecommunications carriers to assist in foreign intelligence surveillance activities and to preserve the secrecy of such surveillance activities.” 50 U.S.C. §§1804(a)(4) and 1805(c)(2). Id. at 21. AT&T also reminds us that the Commission does not have jurisdiction under the Wiretapping and Electronic Surveillance Control Act, 18 Pa.C.S. §§5701-5781, to determine the legality of electronic surveillance. McClellan v. PUC, 634 A.2d 686, 159 Pa. Commw. 675 (1993). Id. at 22-23. Such jurisdiction rests in the court of common pleas, asserts AT&T. Id.

Verizon in its preliminary objections argues that the complaints of ACLU and CWA should be rejected because they: (1) request relief beyond the Commission’s authority to grant; and (2) are legally insufficient. Verizon P.O. at 1. In support of its preliminary objections Verizon, like AT&T, point to the FCC’s refusal to investigate the alleged violations due to the classified nature of the NSA’s activities. Id. at 2. Verizon also notes that it (like AT&T) was

sent a letter by the United States Department of Justice warning it that responding to the New Jersey Attorney General's subpoena "would be inconsistent with and preempted by federal law." Id. at 2-3. Consequently, according to Verizon, because national security is implicated, the Commission will be unable to adduce any facts relating to the claims of ACLU and CWA and thus will be unable to resolve the issues raised in the requests of ACLU and CWA. Id. at 3.

Verizon admits that it "cooperates with national security and law enforcement requests within the bounds of the law." Id. at 6. It argues that "[t]he Wiretap Act, FISA, the Electronic Communications Privacy Act, and the Telecommunications Act all contain exceptions to the general prohibitions against disclosure and expressly authorize disclosure to or cooperation with the government in a variety of circumstances." Id. at 7 (footnote omitted). Verizon also argues that "these laws provide that 'no cause of action shall lie' against those providing assistance pursuant to these authorizations, and also that 'good faith reliance' on statutory authorizations, court orders, and other specified items constitutes 'a complete defense against any civil or criminal action brought under this chapter or any other law.'" Id. (footnotes omitted). Citing Camacho v. Autor. de Tel. de Puerto Rico, 868 F.2d 482, 487-88 (1st Cir. 1989), Verizon asserts that "[t]o the extent that state laws do not contain similar exceptions or authorizations, they are preempted." Id. Verizon opines that an investigation into the matters raised by complainants would require the Commission to interpret and enforce federal statutes governing national security matters, and that the Commission lacks such authority. Id. at 8.

In concluding its argument in support of its preliminary objections, Verizon states as follows:

In sum, there is no basis to assume that Verizon has violated the law. Further, Verizon is precluded by federal law from providing information about its cooperation, if any, with this national security matter. Verizon accordingly cannot confirm or deny cooperation in such a program or the receipt of any government authorizations or certifications, let alone provide the other information [complainants] suggest that the Commission request. As a result, there would be no evidence for the Commission to consider in any investigation. Moreover, neither the federal nor state wiretapping and surveillance statutes authorizes or contemplates investigations or enforcement proceedings by the Commission to determine the lawfulness of any national security

program or of any party's alleged participation in it. Nor does the Commission possess the practical tools and ability to construe and enforce state and/or federal criminal statutes, consistent with all constitutional rights and protections. Accordingly, even if the Commission could inquire into the facts – and as discussed above it cannot – the Commission lacks the authority or jurisdiction to investigate or resolve [complainants'] allegations. Instead, ongoing Congressional oversight through the Senate and House Intelligence committees, as well as the pending proceedings in federal court that will consider the state secrets issues, are more appropriate forums for addressing any issues related to this national security program.

Id. at 8-9.

In its response to the preliminary objections of AT&T and Verizon, ACLU asserts that the Commission does have jurisdiction to hear its complaint. ACLU Response at 6. Citing 66 Pa. C.S. §3019(d) and 52 Pa. Code §63.135(2), ACLU argues that Pennsylvania law expressly protects the privacy of customer information. Id. Section 3019(d) of the Public Utility Code, 66 Pa.C.S. §3019(d), provides:

§3019. Additional powers and duties

* * *

(d) Privacy of customer information.-

(1) Except as otherwise provided in this subsection, a telecommunications carrier may not disclose to any person information relating to any customer's patterns of use, equipment and network information and any accumulated records about customers with the exception of name, address and telephone number.

(2) A telecommunications carrier may disclose such information:

(i) Pursuant to a court order or where otherwise required by Federal or State law.

(ii) To the carrier's affiliates, agents, contractors or vendors and other telecommunications carriers or interexchange telecommunications carriers as permitted by Federal or State law.

(iii) Where the information consists of aggregate data which does not identify individual customers.

66 Pa.C.S. §3019(d) (emphasis supplied).

And Section 63.135(2) of Title 52 of the Pennsylvania Code, 52 Pa. Code §63.135(2), provides:

§ 63.135. Customer information.

This section describes procedures for determining employee access to customer information and the purposes for which this information may be used by employees responding to requests for customer information from persons outside the telephone company and the recording of use and disclosure of customer information.

* * *

(2) Requests from the public. Customer information that is not subject to public availability may not be disclosed to persons outside the telephone company or to subsidiaries or affiliates of the telephone company, except in limited instances which are a necessary incident to:

- (i) The provision of service.
- (ii) The protection of the legal rights or property of the telephone company where the action is taken in the normal course of an employee's activities.
- (iii) The protection of the telephone company, an interconnecting carrier, a customer or user of service from fraudulent, unlawful or abusive use of service.

(iv) A disclosure that is required by a valid subpoena, search warrant, court order or other lawful process.

(v) A disclosure that is requested or consented to by the customer or the customer's attorney, agent, employee or other authorized representative.

(vi) A disclosure request that is required or permitted by law, including the regulations, decisions or orders of a regulatory agency.

(vii) A disclosure to governmental entities if the customer has consented to the disclosure, the disclosure is required by a subpoena, warrant or court order or disclosure is made as part of telephone company service.

52 Pa. Code §63.135(2) (emphasis supplied).

ACLU clarifies that it seeks an investigation into: (1) whether respondents received a request for information; and (2) whether responding to the request would run afoul of Pennsylvania law, as enforced by the Commission. *Id.* at 6-7. ACLU opines that after the Commission resolves those two issues, it can then decide whether ACLU's request for relief is appropriate. *Id.* (In its request for relief included in its complaint, ACLU asks the Commission to order respondents to: (1) provide ACLU and the Commission with a complete accounting of any and all releases of customer information to the NSA or any other federal or state law enforcement agency that was not compelled by court order or warrant; (2) cease and desist from releasing customer calling information to the NSA or other law enforcement agencies without court order or warrant; and (3) take such steps as are necessary to comply with Pennsylvania law.)

ACLU further explains that:

Complainants do not ask the Commission to determine whether the NSA is entitled to make the reported demands for consumer telephone records – indeed, Complainant ACLU has pursued those claims against the NSA in a separate federal court action.

Complainants' primary request in this forum is an "accounting of any and all releases of customer information to the NSA or any other federal or state law enforcement agency that was not compelled by court order or warrant."

Id. at 12.

ACLU argues that by disclosing whether or not they disclosed customer information to the NSA or another U.S. government agency, respondents would not be divulging classified information. Id. at 7. ACLU notes that Qwest Communications Corporation and BellSouth Corporation have divulged that they did not disclose customer information to the NSA, and they have not been prosecuted for the disclosure. Id. ACLU asserts that because the U.S. President has publicly defended the legality of the NSA program, respondents would not be divulging classified information if they disclose whether or not they are participating in the program. Id. at 7-8.

ACLU also argues that respondents refer to inapplicable law in support of their preliminary objections. ACLU notes for example that the Totten rule does not apply in this case because ACLU is not seeking to enforce or interpret terms of an espionage agreement. Id. at 8. ACLU also asserts that the state secrets privilege does not apply in this case because this privilege can only be asserted by a U.S. government department head, and no U.S. government department head has intervened in this case and asserted such a privilege. Id. at 9-10.

In conclusion, ACLU argues that "[t]he complaint before the Commission focuses on the Respondents' conduct, not the NSA's, and is therefore entirely within the jurisdiction of the Commission." Id. at 13-14.

The power of the Commission is statutory; the legislative grant of power to act in any particular case must be clear. City of Philadelphia v. Philadelphia Electric Company, 473 A.2d 997, 1000 (Pa. 1984). The authority of the Commission must arise either from express words of pertinent statutes or by strong and necessary implication therefrom. Id. at 999. The Commission's statutory authority to regulate the rates and service of public utilities that provide service in Pennsylvania is found in the Public Utility Code, 66 Pa.C.S. §§101 - 3316. The Public

Utility Code does not confer upon the Commission an exclusive jurisdiction to decide matters involving regulated public utilities. Virgilli v. Southwestern Pennsylvania Water Authority, 427 A.2d 1251, 1253, 58 Pa. Commw. 340 (1981). For example, as AT&T indicated in its preliminary objections, the Commission does not have jurisdiction over matters involving allegations of illegal wiretapping. McClellan v. PUC, 634 A.2d 686, 688, 159 Pa. Commw. 675 (1993). The Wiretapping and Electronics Surveillance Control Act, 18 Pa.C.S. §§ 5701-5781, gives the courts exclusive power to determine the legality of electronic surveillance. Id.

In the present case, ACLU alleges that AT&T, Verizon and the other telecommunications carriers named in its complaint, may have violated Pennsylvania public utility law (specifically, 66 Pa. C.S. §3019(d)⁶ and 52 Pa. Code §63.135(2)) if they gave the NSA information regarding the calling patterns of Pennsylvania customers without requiring a search warrant or court order before disclosing the information. ACLU asks that the Commission open an investigation into the matter. In such an investigation, ACLU asks that the Commission first compel respondents to admit or deny that they disclosed to the NSA information regarding the calling patterns of Pennsylvania customers, without requiring a search warrant or court order. If respondents answer “yes,” ACLU asks that the Commission then determine whether respondents’ actions violated Pennsylvania public utility law. If the Commission determines that it does, ACLU asks that the Commission then grant its requested relief. The relief requested by ACLU is that respondents be ordered to: (1) provide ACLU and the Commission with a complete accounting of the customer information it provided to the NSA; and (2) cease and desist from providing the information unless a court order or search warrant is produced. ACLU emphasizes that it wants to focus on the conduct of the telecommunications carriers in this proceeding before the Commission, while focusing on the conduct of the NSA in its proceeding before the federal court.

However, in this matter in which the overarching issue of national security has been raised, the conduct of the telecommunications carriers and the conduct of the NSA are inextricably intertwined. Although the complaints are narrowly drawn to test Pennsylvania regulatory authority, the questions involved in this matter are in fact larger in scope than just

⁶ ACLU did not refer to this Statute in its complaint, but it did refer to it in its response to the preliminary objections.

whether the telecommunications carriers, who are the subject of the present complaints, violated the Public Utility Code and Commission regulations. Matters of national security are implicated in this proceeding. There is no indication in the Public Utility Code or the Commission's regulations governing the protection of customer information, that the Pennsylvania Legislature intended that the Commission would decide matters of national security. Nor is there any federal law bestowing such authority upon the Commission. The Commission clearly does not have the experience, expertise and competence to adjudicate cases involving questions of national security. The federal courts however, clearly do have the experience, expertise and competence to handle cases with national security implications.

AT&T and Verizon aver that they are prohibited by federal law governing national security matters from even admitting or denying whether they are providing customer information to the NSA. AT&T and Verizon claim that the U.S. Department of Justice has warned them that their disclosure of whether or not they are participating in any NSA-led surveillance program would be violative of federal law governing national security matters. So as a threshold matter, a determination would have to be made in this case as to whether the Commission has the authority to determine whether or not respondents refusal to comment on whether they are providing customer calling information to the NSA is a matter of national security. And as ACLU indicates, the Commission would first have to determine that the disclosure would not be a matter of national security before it could compel respondents to disclose whether or not they have provided or are providing the NSA with customer calling information. As AT&T and Verizon have noted, the President of the United States, the Director of National Intelligence and the Director of the NSA all say that this is a matter of national security. ACLU says that it is not a matter of national security. ACLU indicates that its interpretation of federal law is that because the United States President has defended the legality of the NSA program, and because other telecommunications carriers have disclosed their non-involvement in the NSA program and have not been prosecuted, AT&T and Verizon would not violate national security restrictions by disclosing whether or not they are involved in the NSA program. However, I agree with Verizon that the Commission does not have the authority to construe and interpret federal law governing national security matters. I therefore find that the Commission does not have the authority to determine whether or not respondents' refusal to

comment on whether they are providing customer calling information to the NSA ^{Page 17 of 21}
national security.

The Commission could not in this case decide the question of whether Pennsylvania public utility law was violated, in a vacuum. It would first be required to compel respondents to divulge whether or not they are providing customer calling information to the NSA. For the reasons provided herein, I find that the Commission does not have the authority to compel respondents to disclose that information over their claims of national security prohibitions.

While complainants allege in this proceeding that respondents possibly violated Pennsylvania public utility law if they provided customer calling information to the NSA without a warrant or court order, the overarching issue is whether any cooperation between the NSA and respondents involving customer calling information was legal consistent with federal law concerning matters of alleged national security. A federal court may provide ACLU with the investigation, determinations and relief that it has requested in its complaint before the Commission. If a federal court decides that the matter of respondents' cooperation or non-cooperation with the NSA in providing customer calling information is a matter of national security, then the inquiry may end there. However, if a federal court decides that it is not a matter of national security or that information may be provided under adequate protections and precautions, then a federal court may: (1) compel respondents to disclose whether or not they are giving the NSA customer calling information without requiring a search warrant or court order; (2) order respondents to provide to ACLU a complete accounting of any customer information respondents provided to the NSA without requiring a search warrant or court order; and (3) order respondents to cease and desist from providing any customer information to the NSA without requiring a search warrant or court order, if the federal court determines that the law requires such a process to be followed. The only aspect of ACLU's complaint that a federal court may or may not address is whether respondents violated Pennsylvania public utility law if they provided customer information to the NSA without requiring a search warrant or court order. However, again, the overarching question is whether federal law was violated if respondents provided customer calling information to the NSA without requiring a search warrant or court order. A federal court, and not the Commission, has jurisdiction to adjudicate that issue. (A case in which

the plaintiffs allege that AT&T is collaborating with the NSA in a massive warrantless surveillance program that illegally tracks the domestic and foreign communication records of millions of Americans, is proceeding in federal court after the federal court denied the motions of the U.S. government and AT&T to dismiss the lawsuit.) See, Hepting, et al. v. AT&T Corp., et al.⁷, Case No. C-06-672 VRW (N.D. Cal.) (July 20, 2006). For all of the foregoing reasons, I will grant the preliminary objections of AT&T and Verizon and dismiss the complaint of ACLU.

Assuming arguendo that the Commission has some decision-making authority in regard to this matter, it would only come after a federal court with binding authority over the Commission, decided: (1) that this is not a matter of national security; (2) that respondents may be compelled to disclose the nature and extent of any customer information they have provided or are providing to the NSA; and (3) that the Commission may decide whether Pennsylvania public utility law was violated if any customer information was provided without a search warrant or court order. If that should occur, then complainants may, if they so choose, file a new complaint based on such a federal court decision.

As earlier noted, ACLU's complaint was also filed against CTSI and InfoHighway. In its answer to the complaint, CTSI avers that it has never been contacted by the NSA and that it has not provided customer calling information to the NSA. InfoHighway's Chairman, Mr. Ginsberg, filed a letter in lieu of an answer to the complaint. In his letter Mr. Ginsberg similarly avers that InfoHighway has: (1) never been contacted by the NSA and asked to provide customer calling information or private calling records for any customer; (2) never provided any information to any governmental agency with respect to any of the account numbers listed in Exhibit B of the complaint; and (3) never provided any information to any governmental authority without being compelled to do so by a valid subpoena or court order. When ACLU received similar answers to its complaint from Denver & Ephrata Telephone & Telegraph Company and Buffalo Valley Telephone Company, albeit those answers were also accompanied by preliminary objections, ACLU withdrew its complaint as to those

⁷ In another federal court case involving similar allegations as in Hepting, but focused on AT&T's Illinois customers, the federal court held that due to the operation of the "states secrets privilege," the plaintiffs could not obtain through discovery the information they needed (regarding any submissions by AT&T of customer calling records to the U.S. government) to prove their standing to sue for prospective relief. The court consequently dismissed the complaint. See, Terkel et al. v. AT&T Corp., et al., Case No. 06 C 2837 (N.D. Ill.) (July 25, 2006).

telecommunications carriers.⁸ See, answers to complaint filed by Denver & Ephraim Telephone Company and Buffalo Valley Telephone Company. The record does not indicate why ACLU has not withdrawn its complaint as to CTSI and InfoHighway. However, because ACLU's complaint against CTSI and InfoHighway, like its complaint against the other remaining respondents, raises matters of national security over which the Commission has no jurisdiction, I will dismiss the complaint as to CTSI and InfoHighway.

In its complaints, CWA alleges that Verizon and AT&T possibly engaged in unreasonable utility practices if they participated in the NSA's "domestic wiretapping program." CWA asks the Commission to open an investigation, and using its "statutory authority" compel respondents to answer questions regarding the nature and extent of their cooperation with the NSA, if any. As previously stated, the Commission does not have jurisdiction over all matters involving regulated public utilities. And as also previously stated, the Commission does not have jurisdiction over matters involving allegations of illegal wiretapping. See, McClellan v. PUC, 634 A.2d 686, 688, 159 Pa. Commw. 675 (1993). Nor does the Commission have jurisdiction over matters of alleged national security, for the reasons stated above. The Commission does not have the authority to determine whether or not respondents' refusal to comment on whether they are providing customer information to the NSA is a matter of national security. Nor does the Commission have the authority to compel respondents to disclose whether or not they have provided or are providing customer information to the NSA. Consequently, the Commission does not have the authority to compel respondent to answer the four questions posed in CWA's complaints regarding the nature and extent of respondents' cooperation with the NSA, if any. Therefore, for all of the foregoing reasons, I will grant the preliminary objections of AT&T and Verizon and dismiss the complaints of CWA.

My dismissal of CWA's complaints, like my dismissal of ACLU's complaints, is without prejudice to the right of CWA to file new complaints if it obtains a federal court decision, that is binding on the Commission, which holds: (1) that this is not a matter of national security; (2) that respondent telecommunications carriers may be compelled to disclose the nature and extent of any customer calling information they have provided to and/or are providing

⁸ The record does not reflect why ACLU withdrew its complaint against United Telephone Company of Pennsylvania d/b/a Embarq Pennsylvania, which did not file an answer to the complaint.

to the NSA; and (3) that the Commission may decide whether Pennsylvania public utility law was violated if any customer calling information was provided without a search warrant or court order.

ORDER

THEREFORE,

IT IS ORDERED:

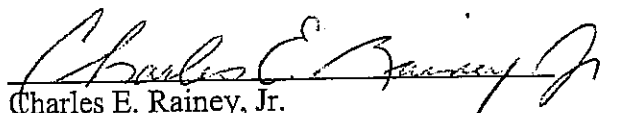
1. That the preliminary objections of AT&T Communications of Pennsylvania LLC are granted.
2. That the preliminary objections of Verizon Pennsylvania Inc., Verizon North Inc. and Verizon Select Services Inc. are granted.
3. That the motion of Verizon Pennsylvania Inc., Verizon North Inc. and Verizon Select Services Inc. for the admission *pro hac vice* of Leigh A. Hyer, Esquire is granted.
4. That the complaint of American Civil Liberties Union of Pennsylvania, et al. against AT&T Communications of Pennsylvania LLC at docket no. C-20066397 is dismissed.
5. That the complaints of American Civil Liberties Union of Pennsylvania, et al. against Verizon Pennsylvania Inc. at docket no. C-20066398, and Verizon North Inc. at docket no. C-20066399 are dismissed.
6. That the complaint of American Civil Liberties Union of Pennsylvania, et al. against CTSI, LLC at docket no. C-20066401 is dismissed.
7. That the complaint of American Civil Liberties Union of Pennsylvania, et al. against ARC Networks Inc. d/b/a InfoHighway Communications at docket no. C-20066404 is dismissed.

8. That the complaints of District 13 of the Communications Workers of America and its Assistant to the Vice President, Terrance T. Tipping, against Verizon Pennsylvania Inc. at docket no. C-20066410, Verizon North Inc. at docket no. C-20066411 and Verizon Select Services Inc. at docket no. C-20066412, are dismissed.

9. That the complaint of District 13 of the Communications Workers of America and its Assistant to the Vice President, Terrance T. Tipping, against AT&T Communications of Pennsylvania LLC at docket no. C-20066413 is dismissed.

10. That the complaints of American Civil Liberties Union of Pennsylvania, et al. and District 13 of the Communications Workers of America and its Assistant to the Vice President, Terrance T. Tipping, are dismissed without prejudice to their right to file new complaints if they should obtain a federal court decision, that is binding on the Commission, which holds: (1) that this is not a matter of national security; (2) that respondent telecommunications carriers may be compelled to disclose the nature and extent of any customer calling information they have provided to and/or are providing to the National Security Agency or other government law enforcement agency; and (3) that the Commission may decide whether Pennsylvania public utility law was violated if any customer calling information was provided without a search warrant or court order.

11. That these cases be marked closed.


Charles E. Rainey, Jr.
Administrative Law Judge

Date: August 16, 2006

STATE OF NEW YORK DEPARTMENT OF PUBLIC SERVICE
THREE EMPIRE STATE PLAZA, ALBANY, NY 12223-1350

Internet Address: <http://www.dps.state.ny.us>

Exhibit 3
Page 1 of 2

PUBLIC SERVICE COMMISSION

WILLIAM M. FLYNN
Chairman
THOMAS J. DUNLEAVY
LEONARD A. WEISS
NEAL N. GALVIN
PATRICIA L. ACAMPORA



DAWN JABLONSKI RYMAN
General Counsel

JACLYN A. BRILLING
Secretary

June 14, 2006

06-19-06P04:13 RCV

Donna Lieberman, ~~Executive Director~~
Corey Stoughton, Staff Attorney
New York Civil Liberties Union
125 Broad Street
New York, New York 10004

Re: New York Civil Liberties Union's Complaint and Request for Investigation
of AT&T and Verizon.

Dear Ms. Lieberman & Mr. Stoughton:

Please accept this letter as my formal response to your correspondence regarding the recent media reports of the alleged cooperation of AT&T and Verizon with the National Security Agency, as well as the Federal Communications Commission's (FCC) actions with respect thereto. As an initial matter, I note that the Public Service Commission of the State of New York takes very seriously the commitment made by the utilities under its jurisdiction to protect the privacy of their customers. In this matter, however, I must inform you that the New York State Public Service Commission respectfully declines to initiate any investigation into the alleged cooperation of AT&T and Verizon with the National Security Agency.

As you may be aware, there is no provision in New York State's Public Service Law specifically concerning the privacy of customer information. Additionally, the existing rules and regulations of the New York State Department of Public Service do not cover activities such as those alleged to have occurred in the recent media reports. On March 22, 1991, in Case 90-C-0075, the Commission released its Statement of Policy on Privacy in Telecommunications. Although that Statement of Policy guides our decisions with respect to our role in overseeing the telecommunication companies under our jurisdiction, the policy statements contained therein do not have the force of law behind them, and, therefore, do not provide this Commission with any authority with which to pursue this matter.

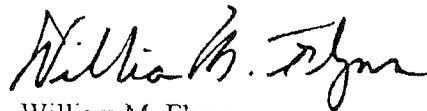
Moreover, in declining to conduct an investigation similar to the one requested in your correspondence, the FCC relied on pleadings submitted by the United States of America in the case of *Hepting v. AT&T*, No. C-06-0672 – VRW (N.D. Cal.). There, the United States asserted

that the "state secrets" privilege applies to any information connected to this matter. The FCC noted that the same privilege would prevent it from ordering the production of classified information or from compelling any parties which they might investigate to respond to their inquiries. Likewise, the Public Service Commission does not have the authority to compel the production of privileged information, nor does it have the jurisdiction required to pass on questions of law surrounding the assertion of such privilege by the United States, Verizon or AT&T. Accordingly, the Public Service Commission is not the correct agency or government entity to conduct the investigation sought in your correspondence.

Finally, even were the Court to decide that the United States is not entitled to the privilege asserted in the *Hepting* case, the Public Service Commission still is not the correct entity to pursue these matters because of their highly sensitive nature and their connection to national security. Therefore, even were such privilege not to apply, the Public Service Commission would still respectfully decline to initiate the investigation you seek.

I thank you again for your correspondence bringing this matter to our attention. Please feel free to contact me in the future if you have any additional concerns as they relate to the New York State Public Service Commission.

Sincerely,



William M. Flynn
Chairman

cc: Kevin Martin, Chairman, Federal Communications Commission
Ivan Seidenberg, Chairman & CEO, Verizon
William Barr, Executive Vice President & General Counsel, Verizon
Edward Whitacre, Chairman, AT&T
Randall Stephenson, Chief Operating Officer, AT&T
Keefe B. Clemons, Associate General Counsel – NY & CT, Verizon

OFFICE OF THE GENERAL COUNSEL
P.O. Box 1197
Richmond, Virginia 23218-1197

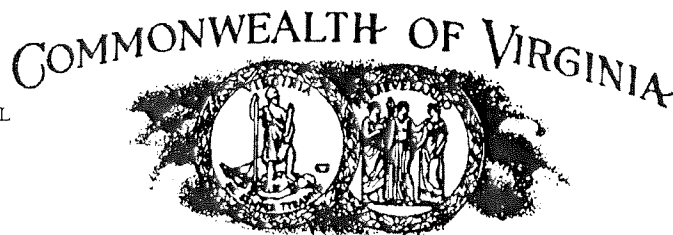


Exhibit 4
Page 1 of 1

Telephone Number (804) 371-9671
Facsimile Number (804) 371-9240
Facsimile Number (804) 371-9549

STATE CORPORATION COMMISSION

June 1, 2006

ACLU of Virginia
530 East Main Street
Suite 310
Richmond, Virginia 23219

ATTN: Kent Willis
Executive Director

Rebecca K. Glenberg
Legal Director

RE: Letter complaint dated May 24, 2006

Dear Mr. Willis and Ms. Glenberg:

Your letter complaint dated May 24, 2006, was received via telefax in the State Corporation Commission's Division of Communications ("Division"). At the request of the Division's Director, William Irby, I have reviewed your communication. You have requested that the State Corporation Commission ("Commission") undertake an investigation of "Verizon," citing a press story in the May 11, 2006, edition of *USA Today* as a basis. However, your letter complaint identifies no provision of Virginia law, nor any rule or regulation administered by or under the jurisdiction of the Commission, that "Verizon" is alleged to have violated. In addition, your letter does not identify actions that the Commission can take – within its jurisdiction – to resolve the matters raised in your letter, nor am I aware of any action the Commission could undertake to resolve these matters.

Therefore, on my advice, the Commission's Staff declines to initiate the requested investigation.

Very truly,

A handwritten signature in cursive script, appearing to read "William H. Chambliss".
William H. Chambliss
General Counsel

WHC:ncl

cc: William Irby

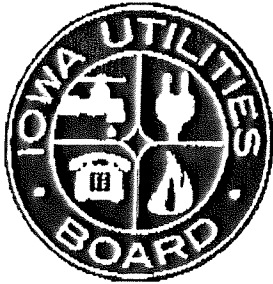


Exhibit 5
Page 1 of 1

THOMAS J. VILSACK, GOVERNOR
SALLY J. PEDERSON, LT. GOVERNOR

JOHN R. NORRIS, CHAIRMAN
DIANE MUNNS, BOARD MEMBER
CURTIS W. STAMP, BOARD MEMBER

May 25, 2006

Frank Burnette
802 Insurance Exchange Building
505 Fifth Avenue
Des Moines, Iowa 50309-2317

Dear Mr. Burnette:

I am in receipt of your letter of May 22, 2006, asking the Iowa Utilities Board to investigate the actions of AT&T and Verizon Cellular with respect to allegations that those companies, and others, have provided the National Security Agency with access to certain information. Unfortunately, the Board does not have jurisdiction to conduct such an investigation; the services you describe are deregulated in Iowa.

Specifically, Iowa Code § 476.1D requires that the Board deregulate communications services that are subject to effective competition. Pursuant to that statutory duty, the Board has deregulated the long distance services provided by AT&T and the mobile communications services provided by Verizon. Long distance was deregulated in two steps, in 1989 and 1996, and mobile telephone service was deregulated in 1986.

When services are deregulated, "the jurisdiction of the board as to the regulation of [those] communications services is not applicable...." (Iowa Code § 476.1D(1).) Thus, the Board does not have jurisdiction to conduct the investigation you request.

I hope you find this information helpful. If you have any comments or questions concerning this matter, please feel free to contact me at my direct number, 515-281-8272, or by email at david.lynnch@iub.state.ia.us.

Sincerely,

A handwritten signature in black ink, appearing to read "David J. Lynch".

David J. Lynch
General Counsel

Cc:
Iowa Civil Liberties Union
Qwest Corporation

BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF DELAWARE

IN THE MATTER OF THE REQUEST OF TEN)
CUSTOMERS TO INITIATE AN INVESTIGATION)
INTO WHETHER VERIZON DELAWARE INC. AND) PSC DOCKET NO. 06-179
AT&T COMMUNICATIONS OF DELAWARE, LLC,)
HAVE IMPROPERLY SHARED TELEPHONE RECORDS)
(FILED MAY 25, 2006))

ORDER NO. 6965

This 11th day of July, 2006, the Commission determines and Orders the following:

1. Ten Delawareans, all customers of "Verizon," have filed a complaint (see 26 Del. C. § 207) asking the Commission to exercise its discretion to open an investigation. The inquiry would be to find out if "Verizon" or "AT&T" has been supplying federal intelligence agencies with information about who its customers are calling, either by providing customer call record data or by granting the federal agencies network access to such call data. If it turns out that either carrier has been passing call information, complainants ask the Commission to then determine whether Verizon and AT&T have acted legally: did they have a legal basis for providing, or allowing the mining of, such customer calling information?¹ By a subsequent submission, 110 other residents endorse the call for a Commission investigation.

¹As for the scope of the legality inquiry, complainants allege facts that may constitute violations of Delaware law governing: (1) deceptive trade practices; and (2) electronic surveillance, stored wire and electronic communications, and transactional record access. See 6 Del. C. §§ 2531-2536; 11 Del. C. §§ 2401-2412, 2421-2427. In response, AT&T argues that federal law preempts this Commission from investigating the ACLU's allegations, noting that several federal statutes prohibit the disclosure of classified information, that the United States has invoked the Military States Secrets Privilege to ensure

2. AT&T and Verizon (in the guise of Verizon Delaware Inc.) have each informally responded. Both carriers assert that because the Director of National Intelligence and the Director of the National Security Agency have claimed that information regarding federal anti-terrorism programs is classified, the carriers are barred from disclosing (or even discussing) what each has done (or not done), what data might (or might not) be flowing to the federal intelligence agencies, and what "legal" justifications support the carrier's actions, or the government's demands or requests. As AT&T paints it, if the carriers cannot (because of federal statutes and Executive Orders) tell anything, then there is little to be gained by the Commission asking. Any inquiries from this Commission would be met with silence from the carriers, given the criminal sanctions that attach under federal laws for disclosure of classified information.²

3. Anyone that reads, or listens, to the news knows that the crux of the filed complaint is not a Delaware-only controversy. Telephone subscribers in more than twenty other jurisdictions have filed complaints with their state utility commissions or Attorney Generals asking for investigations about what customer call data is flowing to federal intelligence agencies. In addition, several class action lawsuits are pending throughout the country, challenging carriers' alleged

that there is no disclosure of the information at issue here, and that the United States sued state officials and carriers to prevent disclosure of this information through state subpoenas.

²Chairman Martin of the Federal Communications Commission ("FCC") has said that these invocations of national security secrecy - as they would displace any authority that the FCC normally would have to compel information from the carriers - preclude any FCC investigation whether carriers might be violating the provisions of 47 U.S.C. § 222 by providing customer proprietary network information to federal intelligence agencies. Letter of K. Martin, FCC Chair to Hon. E. Markey, Ranking Member (May 22, 2006).

participation in the transfer of customer calling information to the National Security Agency and other intelligence bodies.³ And in those cases, the federal government has invoked the powers assigned to it by the Constitution to conduct war and foreign relations as grounds to bar any inquiry into the carriers' actions and the government's surveillance methods.⁴

4. After hearing from the parties on June 20, 2006, the Commission believes that, in the present context, it is appropriate to suspend any further action in this matter for six months. The complaint and the carriers' responses pose questions of the highest magnitude. The courts are better equipped, in both resources and expertise, to assay the competing claims of customers' statutory rights of privacy and the needs of national security. Within six months, rulings from the federal District Courts, if not Courts of Appeal (or even the Supreme Court), might give a better picture concerning whether the federal government's concerns of national security justify an all-encompassing blanket of secrecy. Once the courts have moved forward on that threshold question, the Commission can better discern whether there can exist room for any investigation by a state utility commission.

5. One additional caution. The six-month suspension should not be read as a commitment by the Commission that it will undertake an

³See, e.g., Hepting v. AT&T Corp., No. C-06-0672 VRW (N.D. Cal.).

⁴In particular, the federal government is now seeking to enjoin subpoenas issued by the Attorney General of New Jersey that seek information about AT&T, Verizon, and other carriers disclosing calling information related to customers in that State. The federal government asserts that the federal war-making and foreign relations powers preempt any inquiry by a State officer seeking to enforce State law dictates. United States v. Zulima v. Farber, et al., Civ. Action No. 3:06 cv 02683-SRC-TJB (D. N.J.) (filed June 14, 2006).

investigation if the courts find some form of disclosure allowable. The Commission is simply suspending any decision on whether to initiate an investigation until the threshold issues of whether information will or will not be available is sorted out in the judicial fora.

Now, therefore, **IT IS ORDERED:**

1. That proceedings in this matter, resulting from the petition or complaint filed by Helen K. Foss, Enno Krebbers, Phyllis Levitt, Lawrence Hamermesh, Marion Hamermesh, Judith Mellen, Joy Mulholland, Gilbert Sloan, Sonia Sloan, and Serena Williams on May 26, 2006, are hereby held in abeyance for a period of six months from the date of this Order. After such time, the complainants can ask the Commission to revisit this matter to determine whether to initiate an investigation under 26 Del. C. § 207.

2. That the Commission reserves the jurisdiction and authority to enter such further Orders in this matter as may be deemed necessary or proper.

BY ORDER OF THE COMMISSION:

/s/ Arnetta McRae
Chair

/s/ Joann T. Conaway
Commissioner

/s/ Jaymes B. Lester
Commissioner

PSC Docket No. 06-179, Order No. 6965 Cont'd.

/s/ Dallas Winslow
Commissioner

/s/ Jeffrey J. Clark
Commissioner

ATTEST:

/s/ Karen J. Nickerson
Secretary

STATE OF COLORADO

Exhibit 7

Page 1 of 4

PUBLIC UTILITIES COMMISSION

Gregory E. Sopkin, Chairman
Polly Page, Commissioner
Carl Miller, Commissioner
Doug Dean, Director

Department of Regulatory Agencies
Tambor Williams
Executive Director



Bill Owens
Governor

August 23, 2006

Mr. Taylor Pendergrass, Esq.
American Civil Liberties Union of Colorado
400 Corona Street
Denver Colorado 80218-3915

Dear Mr. Pendergrass:

Thank you for your faxed letter of August 18, 2006 requesting that the Colorado Public Utilities Commission ("PUC") go forward with an investigation as to whether certain telephone service providers under the PUC's jurisdiction provided information to the National Security Agency ("NSA"). I appreciate your interest in PUC matters; however, it remains my belief that an investigation into this issue is not warranted at this time.

You indicate in your letter that the PUC relied on the pendency of a federal government motion to dismiss in the case of *Hepting v. AT&T Corp.*, No. C06-0672-VRW (N.D. Cal.), before determining whether to proceed with an investigation. While you state that the matter in *Hepting* was resolved when the court refused to dismiss the lawsuit, it is my understanding that Judge Walker nonetheless stayed the case pending an appeal to the 9th Circuit Court of Appeals. It would appear that the matter is in fact not finally resolved.

Of more concern is the matter of *ACLU v. National Security Agency*, Case No. 06-CV-10204, (E.D. Mich. 2006) (order issued August 17, 2006). There, the court, while finding for Plaintiffs on the state secrets privilege defense with regard to warrantless wiretapping, nonetheless dismissed Plaintiff's data-mining claims. The court found that the ACLU could not sustain its data-mining claims without the use of privileged information and further litigation would force the disclosure of the very information the privilege is designed to protect. As you are aware, the PUC's jurisdiction does not extend to the adjudication of constitutional or tort claims. The matters which you urge the PUC to investigate are directly related to the data-mining claims dismissed by the federal court in Michigan. Since the data-mining issue may be the only claim the PUC could proceed under at this time and the same claim has been dismissed by the Michigan court, I disagree that any "green light" has been given by the federal courts..

1580 Logan Street, Office Level 2, Denver, Colorado 80203, 303-894-2000


www.dora.state.co.us/puc
Permit and Insurance (Outside Denver) 1-800-888-0170
TTY Users 711 (Relay Colorado)
Consumer Affairs 303-894-2070

Consumer Affairs (Outside Denver) 1-800-456-0858
Hearing Info 303-894-2025
Transportation Fax 303-894-2071
Fax 303-894-2065

Based on this information, it remains my determination that it would be imprudent of the PUC to expend scarce taxpayer money and PUC resources in an investigation that may yet be preempted and rendered moot by national security interests. Consequently, the PUC will not conduct an investigation at this time, but will instead await a definitive ruling from the federal courts regarding a state public utility commission's authority to investigate such matters.

Thank you very much for your interest in this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Doug Dean", written in a cursive style.

Doug Dean
Director

STATE OF COLORADO

PUBLIC UTILITIES COMMISSION

Gregory E. Sopkin, Chairman
Polly Page, Commissioner
Carl Miller, Commissioner
Doug Dean, Director

Department of Regulatory Agencies
Tambor Williams
Executive Director



Bill Owens
Governor

June 19, 2006

Mr. Taylor Pendergrass, Esq.
American Civil Liberties Union of Colorado
400 Corona Street
Denver, Colorado 80218-3915

Dear Mr. Pendergrass:

Thank you for your letter of May 24, 2006 requesting a Colorado Public Utilities Commission ("PUC") investigation into disclosure of customer proprietary network information ("CPNI") by various telecommunications providers to the National Security Agency ("NSA"), as reported in the May 11, 2006 of *USA Today*.

After reviewing the matter carefully and conferring with our legal counsel, it is my determination that an investigation by the PUC is not warranted at this time. While you interpret various PUC rules and Colorado statutes in your letter as providing that the PUC has jurisdiction to investigate this matter, it is my opinion that current activities by the federal government require that the PUC defer any action at this time.

For example, the activities at issue are currently the subject of a court action in the United States District Court for the Northern District of California. See, *Hepting v. AT&T Corp.*, No. C06-0672-VRW (N.D. Cal.). That matter directly deals with the issues you raise in your letter, specifically, whether the NSA gained access to various telecommunications providers' CPNI records. It is my understanding that the federal government has intervened to dismiss that action on the basis of the military and state secrets privilege.

Additionally, it has come to my attention that the New Jersey Attorney General has issued subpoenas to several telecommunications providers to determine whether any of them violated New Jersey's consumer protection laws by providing CPNI to the NSA. However, the U.S. Department of Justice has filed a lawsuit in the United States District Court in New Jersey in that matter to block the subpoenas. The Department of Justice's action sets the stage to determine the extent of a state's power in this matter over the federal government's national security powers and their

1580 Logan Street, Office Level 2, Denver, Colorado 80203, 303-894-2000

www.dora.state.co.us/puc
Permit and Insurance (Outside Denver) 1-800-888-0170
TTY Users 711 (Relay Colorado)
Consumer Affairs 303-894-2070

Consumer Affairs (Outside Denver) 1-800-456-0858
Hearing Info 303-894-2025
Transportation Fax 303-894-2071
Fax 303-894-2065

Mr. Taylor Pendergrass
Page 2

preemptive effective over state authority. The Department of Justice has asserted that New Jersey, and all states, stray into federal matters when they assert authority over telecommunications providers in matters that involve national security.

Given the two above mentioned matters, I have determined that it would be imprudent of the PUC to expend scarce taxpayer money and PUC resources at this time in an investigation that may be preempted and rendered moot by national security interests. Consequently, the PUC will not conduct an investigation at this time, but will instead await a definitive ruling from the United States District Courts regarding a state's authority to investigate such matters.

Again, thank you very much for your interest in this matter.

Sincerely,

A handwritten signature in black ink that reads "Doug Dean". The signature is written in a cursive, slightly slanted style.

Doug Dean
Director

[Service Date September 27, 2006]

**BEFORE THE WASHINGTON STATE
UTILITIES AND TRANSPORTATION COMMISSION**

In the Matter of:

AMERICAN CIVIL LIBERTIES UNION
OF WASHINGTON

Petition for Investigation

DOCKET NO. UT-060856

ORDER 02

ORDER OPENING AND
DEFERRING INVESTIGATION
PENDING RESOLUTION OF
FEDERAL ISSUES; DIRECTING
TELECOMMUNICATIONS
COMPANIES TO PRESERVE
RECORDS

I. SUMMARY

1 This docket involves a claim that telecommunications companies offering intrastate telecommunications services in this state have violated WAC 480-120-202, and/or other laws and other rules of the Washington Utilities and Transportation Commission (Commission), by unlawfully providing private customer calling information to the federal government.

2 The Commission has received comments¹ from several interested persons recommending various courses of action including: (1) open an informal investigation;² (2) institute a formal complaint for violations of Commission laws and rules;³ or (3) await final resolution of federal issues identified in this docket, that are currently pending in the federal courts.⁴

¹ We use the generic term “comments” to cite the written comments, though the comment documents often use different terms.

² *E.g.*, Comments of ACLU (June 30, 2006) at 8; Comments of David E. Griffith (June 30, 2006) at 3; Comments of Senator Kohl-Welles (June 30, 2006); Comments of Representative Upthegrove (June 27, 2006).

³ *E.g.*, Comments of Stephen Gerritson and Michele Spencer (June 20, 2006) at 2; Comments of Laurie A. Baughman (June 30, 2006) at 5.

⁴ *E.g.*, Comments of Public Counsel (June 30, 2006) at 56-57. This is consistent with the comments of AT&T and Verizon, which assert that the Commission can do nothing because federal law bars the companies from providing information to the Commission. *E.g.*, Comments of AT&T (May 26, 2006) at 10; Comments of Verizon (June 30, 2006) at 8-9. If the federal courts rule to the contrary, the Commission would seem to be free to pursue violations.

3 For reasons explained below, we open an investigation but defer further action pending final
resolution of the federal issues by the federal courts. Meanwhile, all telecommunications
companies offering intrastate wireline telecommunications services in this state are directed
to preserve relevant records and we address the statute of limitations in order to preserve our
jurisdiction.

II. INTRODUCTION

4 Like many state regulatory agencies and the Federal Communications Commission (FCC),
the Commission has promulgated rules designed to protect the privacy of information
regarding a customer's telephone use. Protected information includes the duration of the
call, the person called, and type of call. This information is commonly referred to as
"Customer Proprietary Network Information," or CPNI.⁵

5 Specifically, the Commission has adopted WAC 480-120-202, which in turn adopts the
privacy safeguards for CPNI adopted by the FCC in 47 C.F.R. §§ 64.2003 through 2009.⁶ In
general, the effect of WAC 480-120-202 is to prevent telecommunications companies⁷ that
provide intrastate wireline telecommunications services to Washington customers from
providing CPNI to third parties, except with the customer's consent or as otherwise
permitted or required by law or rule.⁸

6 The Commission opened this docket on May 25, 2006, upon receiving a request from the
American Civil Liberties Union of Washington (ACLU). The ACLU asked the Commission
to investigate whether telecommunications companies violated Commission laws and rules
by unlawfully releasing CPNI to the federal government.⁹

⁵ CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." *WAC 480-120-202, adopting by reference 47 C.F.R. § 64.2003, which adopts this definition of CPNI found in 47 U.S.C. § 222(h)(1).*

⁶ The Commission notes that the FCC has declined to investigate the same matters at issue in this docket. *See* Comments of AT&T (June 30, 2006), Attachment G, Letter from FCC to Representative Markey (May 22, 2006).

⁷ In general, the Commission regulates companies offering intrastate telecommunications services: *i.e.*, telecommunications services between points in the state of Washington. The Commission does not regulate companies that provide exclusively interstate telecommunications services, nor the interstate services of companies that also provide intrastate services in this state.

⁸ *See also* 47 U.S.C. § 222(c)(1): telecommunications companies may not divulge CPNI except "as required by law or with the approval of the customer."

⁹ ACLU request (May 23, 2006) at 4.

7 The ACLU bases its request on reports contained in national news publications stating that Verizon, AT&T, and perhaps other telecommunications companies, have released information to the federal National Security Agency (NSA), without lawful authority. Based on these press reports, the ACLU argues that the Commission should open an investigation into the activities of several telecommunications companies operating in Washington to determine whether any unlawfully released CPNI and if so, to pursue violations of Commission laws and rules.¹⁰

III. PROCEDURE

8 This matter first came before the Commission at its open meeting on July 12, 2006. The Commission deferred action pending receipt of additional comments and information solicited by the Commission from interested persons. At the Commission's open meeting on August 30, 2006, the Commission acknowledged receipt of additional written comments, and oral comments were presented by ACLU, AT&T, Verizon and Public Counsel. Attorneys from the Utilities and Transportation Division of the Attorney General's Office responded to specific questions from the commissioners.

9 The Commission again decided to defer action, pending receipt of additional comments and information by September 6, 2006. Written comments were filed by, among others, the Public Counsel Section of the Attorney General Office, AT&T, Verizon, and the Washington Independent Telephone Association (WITA).

10 This matter came before the Commission at its September 27, 2006, open meeting for deliberation by the commissioners. At that meeting the Commission made the decisions expressed in this order.

IV. DISCUSSION

11 The threshold legal issues here are matters of federal law and are pending before many commissions and in more than 30 court cases filed across the country.¹¹

¹⁰ *Id.* at 1-4.

¹¹ *E.g.*, Comments of AT&T (June 30, 2006) at 3. The federal court system has responded to this large number of federal cases involving essentially the same issues. On August 9, 2006, 16 cases from various federal district courts were consolidated with *Hepting v. AT&T Corp.*, Case No. C 06-0672-VRW, which is currently pending before the District Court for the Northern District of California. See MDL Docket No. 1791, *In re National Security Agency Telecommunications Records Litigation*, Transfer Order (August 9, 2006). More cases may be consolidated.

A. Substantial federal legal issues currently pending in the courts need to be resolved

- 12 A major issue presented is whether the “state secrets” privilege bars telecommunications companies from disclosing whether they have provided CPNI to the federal government.¹² AT&T and Verizon argue that they cannot divulge their relationship, if any, with the NSA without committing a felony.¹³ They also claim that telecommunications companies are required by statute to cooperate with the federal government in these matters, and are immune from lawsuits when they do so.¹⁴ Moreover, they contend the Commission is preempted by federal law from taking any action in this matter.¹⁵ These legal arguments are contested or questioned by other commenters.¹⁶
- 13 Where these issues have been joined in other jurisdictions, a clear and consistent pattern has emerged: When a case is presented before a court or a commission in which a telecommunications company is asked to state whether it provided CPNI to the NSA, the United States Department of Justice has filed a lawsuit in federal court to prevent the company from providing that information, and/or to prevent the state commission from obtaining that information.¹⁷
- 14 Although most of the cases have arisen by means of customer complaint in federal court, recent events in the state of Missouri provide a typical example of how the federal government has acted to protect its interests when a state agency seeks to investigate such matters.
- 15 In June 2006, two members of the Missouri Public Service Commission issued subpoenas to AT&T, asking for specific information about AT&T's involvement with the NSA telephone surveillance program. AT&T declined to produce the records, and the two commissioners

¹² *E.g.*, Comments of AT&T (May 26, 2006) at 2-4, and the legal pleadings attached to those Comments (Attachments A, C, D and F); Comments of AT&T (June 30, 2006) at 1-4 and 9-10 and the legal pleading and correspondence attached to those Comments (Items A, B and C); Comments of Verizon (June 30, 2006) at 1 and 3-5 and 7-8, and the pleading and correspondence attached to those Comments as Exhibits 1, 2, 3, 9 and 10.

¹³ *Id.*

¹⁴ *E.g.*, Comments of AT&T (May 26, 2006) at 5, citing 18 U.S.C. §§ 2511(1), 2511(3), 2520(d), 2702(b), (c) & (e), 2703, 2709, 3124(d) & (e); 50 U.S.C. § 1805(f) & (i), 1842(f), and 1843; Comments of AT&T (June 30, 2006) at 3; Comments of AT&T (July 17, 2006) at 2-3; Comments of Verizon (July 17, 2006) at 4-5.

¹⁵ *E.g.*, Comments of Verizon (June 30, 2006) at 3-4, 6; Comments of Verizon (July 17, 2006) at 2-5; Comments of AT&T (June 30, 2006) at 4-9; Comments of AT&T (July 17, 2006) at 4-5.

¹⁶ *E.g.*, Comments of ACLU (June 30, 2006) at 2-5 and 7-8; Comments of Public Counsel (June 30, 2006) at 54; Comments of David A. Griffith (June 30, 2006) at 1-2; Comments of Stephen Gerritson and Michele Spencer (June 20, 2006) at 2; Comments of Laurie A. Baughman (June 30, 2006) at 1-2 and 4.

¹⁷ This pattern is also noted in the Comments of AT&T (August 25, 2006) at 2 and Comments of Verizon (August 29, 2006) at 2.

went to court to compel compliance with the subpoenas. On July 25, 2006, the Department of Justice filed a lawsuit in federal district court in St. Louis to bar such disclosure. That lawsuit is pending.

- 16 Based on the comments filed by AT&T and Verizon in this docket, these companies will continue to assert, among other things, that federal law bars them from providing information surrounding any disclosure of CPNI to the federal government, even to state whether or not they provided CPNI to the federal government.¹⁸
- 17 It is also clear that the federal legal issues presented in this docket are pending in the federal courts. One such case is *Hepting v. AT&T Corp.*, Case No. C 06-0672-VRW, which is being tried in the federal district court for the Northern District of California. That court, like those in Washington state, is in the Ninth Circuit.
- 18 Consequently, absent strong countervailing considerations directly impairing the public interest, it is not prudent for the Commission to try to resolve these issues now, because ultimately the federal courts will decide them. If the Commission were to investigate or issue a complaint, there can be no reasonable doubt the Commission would be sued in federal court and enjoined from requiring the companies to supply information about whether they provided CPNI to the federal government until the underlying constitutional, national security, and related legal issues have been determined by the federal courts.
- 19 Under these circumstances, we agree with Public Counsel that it makes more sense to await final resolution of these federal legal issues before taking action.¹⁹

¹⁸ See, e.g., Comments of AT&T (June 30, 2006) at 2 and 6; Comments of AT&T (July 17, 2006) at 2 and 6-7, and Exhibit A attached to those comments.

¹⁹ E.g., Comments of Public Counsel (July 17, 2006) at 7-11. This same conclusion has been reached by at least two other commissions, in the same or substantially similar circumstances: the Colorado Public Utilities Commission and the Delaware Public Service Commission.

The Colorado Commission stated that “the PUC will not conduct an investigation at this time, but will instead await a definitive ruling from the federal courts regarding a state public utility commission’s authority to investigate such matters.” See Comments of Verizon (August 23, 2006), Exhibit 2, Letter from Colorado Public Utilities Commission Director to ACLU (August 23, 2006) at 2.

The Delaware commission decided to defer action for at least six months, pending court developments. As Delaware Commissioner Clark stated: “in the end, this is going to be decided in the Federal Courts, since it is going to be a Federal preemption and Federal privilege issue. So, for us to be out in front of it in a situation where in another jurisdiction they are going to have to make a decision whether or not this issue can go forward, I don’t think that is a position that, at least at this stage, I feel comfortable asserting ourselves into.” See Comments of AT&T (June 30, 2006), Exhibit G, Transcript in Docket 06-179 (Delaware Public Service Commission, June 20, 2006), at TR. 35, lines 15-23.

B. Other considerations

20 In making this decision, we identify three concerns that must be addressed: (1) whether the statute of limitations is tolled; (2) whether there would be a sufficient basis for issuing a complaint; and (3) whether telecommunications companies will retain relevant records.

1. Statute of limitations

21 If we await final resolution of the federal issues before taking action, a telecommunications company may argue that the statute of limitations has run on any Commission complaint.²⁰ The applicable limitations period for a penalty action in this context appears to be two years. *RCW 4.16.100(2)*.²¹ The time it may take to resolve the federal legal issues could be two years, or longer. Consequently, if there were violations, companies could respond that expiration of the limitation period had foreclosed the Commission's legal ability to issue penalties.

22 We believe the statute of limitations will not bar future Commission penalties if the resolution of the federal issues allows such action. The Commission asked AT&T and Verizon to waive the statute of limitations pending final resolution of the federal issues that apply in this case.²² AT&T has agreed to do so.²³ We accept AT&T's waiver.²⁴

23 Verizon on the other hand, asserts that this issue is "premature."²⁵ However, at the Commission's August 30, 2006, open meeting, Verizon's counsel acknowledged the nature of the alleged violations and that the legal bars Verizon asserted foreclose Commission action at this time. These legal bars make information relevant to determining whether Verizon violated Commission laws and rules unavailable to the Commission. In this context we believe the "discovery rule" applies.

24 Under the discovery rule, "a cause of action does not accrue until an injured party knows, or in the exercise of due diligence should have discovered, the factual bases of the cause of

²⁰ Nothing in this order constitutes a Commission decision that any telecommunications company has violated any Commission rule, or that the Commission would issue a penalty, if the Commission found such a violation occurred. These decisions must await a future complaint, if any, based on the record to be developed at that time.

²¹ The issue of the applicable limitations period has not been briefed by the parties. The Commission has not made a final decision on this issue, and we do not decide this issue here.

²² *Notice of Further Opportunity to Comment* (August 25, 2006), at 2, Question 1.

²³ Comments of AT&T (August 29, 2006) at 1-2.

²⁴ The Commission does not accept AT&T's reservations, which will be addressed in the future, if necessary.

²⁵ Comments of Verizon (August 29, 2006) at 2-3.

action.”²⁶ In other words, the discovery rule “tolls” the statute of limitations that might otherwise apply. Whether the court will apply the discovery rule in a specific case is based on a balancing test: “[T]he possibility of stale claims must be balanced against the unfairness of precluding justified causes of action.”²⁷

25 Verizon clearly asserts a legal bar to any Commission attempt to discover the relevant facts surrounding any disclosure of CPNI to the federal government which might give rise to a cause of action. It is equally clear that the federal government would take legal action to bar such disclosure.

26 In these circumstances we believe the balance favors tolling the statute against Verizon. Verizon knows the nature of the claims that might be asserted and can protect against “staleness” in its defense should it choose to do so. The Commission, on the other hand, by Verizon’s own argument cannot proceed at present.

2. Basis for a complaint

27 Another consideration is whether the Commission has a sufficient basis for initiating a complaint. Under WAC 480-120-202 the Commission has jurisdiction over telecommunications carriers offering intrastate wireline services in this state. So far, no information has been brought to the Commission’s attention that would tend to show the existence of any disclosure of CPNI to the federal government that is related to Washington intrastate telecommunications.

28 Public Counsel observes that “it would be extremely difficult, even from publicly available materials, for the Commission to make an adequate factual record until the federal issues are resolved.”²⁸ Given the information before us, this most likely is an understatement.

29 The information cited by the ACLU consists of uncorroborated newspaper reports that are not specific to Washington intrastate telecommunications. The ACLU, AT&T and Verizon all agree that uncorroborated newspaper reports do not constitute probable cause for a complaint proceeding.²⁹

²⁶ *In re Estates of Hibbard*, 118 Wn.2d 737, 744, 826 P.2d 690 (1992).

²⁷ *U.S. Oil v. Dep’t of Ecology*, 96 Wn. 2d 85, 93, 633 P.2d 1329 (1981).

²⁸ Comments of Public Counsel (July 17, 2006) at 11.

²⁹ Comments of ACLU (August 29, 2006) at 1; Comments of AT&T (August 29, 2006) at 2-3; Comments of Verizon (August 29, 2006) at 3-4.

30 On the other hand, the Commission routinely investigates telecommunications companies for compliance with Commission laws and rules. The Commission conducts audits and provides technical assistance or other measures as may be required to provide incentives to comply. The Commission does not need to make a finding of probable cause that a violation has occurred before conducting such investigations.

31 Public Counsel argues that an administrative agency has wide discretion regarding when it will take action, and that “probable cause” is not the minimum standard for agency complaints or investigations.³⁰ We agree with Public Counsel. Regardless of the legal standard for initiating a complaint or an investigation, however, it would not be productive to do so now for the reasons previously discussed. Any complaint or investigation should await a determination in the federal courts that such a proceeding is lawful.

3. Retention of relevant information

32 By not proceeding now, there is some risk that relevant information now possessed by or known to telecommunications companies may not be preserved until the federal issues are resolved.

33 AT&T and Verizon state they are bound to retain this information under the civil litigation in which they are currently involved.³¹ We have no basis for taking issue with these statements; however, we have no say in how that litigation may address document retention relevant to our potential future jurisdiction. Further, we do not know whether other companies subject to our jurisdiction that may not be parties to pending federal court litigation possess relevant information.

V. DECISION

34 For the reasons stated above, we decline to issue a complaint or begin an active investigation at this time of possible violations of WAC 480-120-202 and/or other Washington laws or Commission rules.

35 However, we find it necessary to ensure that relevant information is preserved that will enable a later Commission investigation, should such be permitted by the courts. Therefore, we direct the Secretary to open an investigation docket on this matter, and direct every telecommunications company offering intrastate wireline telecommunications services in this state to retain information about any approach by or on behalf of the federal government

³⁰ Comments of Public Counsel (September 6, 2006).

³¹ Comments of AT&T (August 29, 2006) at 4; Comments of Verizon (August 29, 2006) at 4.

to provide CPNI. Each company must preserve all records and information about any such request and the information provided, until further order of the Commission. If any current or former company official or employee has personal knowledge of any such information, the company is directed to retain the name of the person, the nature of the information she or he possesses, and the last known contact information for the person. The provisions of CPNI subject to this order are those associated with Washington intrastate telecommunications provided by wireline carriers. The order shall make clear the nature of the allegations, and that each telecommunications company should assume, for purposes of notice and information retention purposes, that the allegations may apply to them.

36 If the courts bar any state action for violations of rules such as WAC 480-120-202 or other relevant laws and Commission rules, the investigation docket will be closed and the document retention directive will be withdrawn.

37 If the courts allow state investigations into these issues, the Commission will determine further appropriate action at that time.

38 From the foregoing findings, the Commission makes the following conclusions of law:

CONCLUSIONS OF LAW

39 Based on the written and oral record in this docket and on the foregoing discussion, the Commission makes the following conclusions of law:

- 40 1. The Commission has jurisdiction over the practices of telecommunications companies offering intrastate wireline telecommunications services in this state, which are subject to the provisions of WAC 480-120-202, regarding the privacy protections for customer proprietary network information (CPNI).
- 41 2. Claims that telecommunications companies violated WAC 480-120-202, and/or any other Commission laws and rules, by unlawfully providing CPNI to the federal government raise predicate issues of federal law which must be resolved by federal courts before the Commission can meaningfully conduct an investigation or pursue a complaint.
- 42 3. Judicial economy warrants waiting for the final resolution of the federal legal issues already pending in federal courts before taking further action to investigate claims raised in this docket.

- 43 4. In order to preserve relevant evidence that may currently exist until such time as the federal legal issues are resolved and the Commission can determine whether to investigate or file a complaint in this matter, it is necessary to enter a protective order.
- 44 5. In order to preserve the Commission's jurisdiction to assess penalties until such time as the federal legal issues are resolved and the Commission can determine whether to investigate or file a complaint in this matter it is necessary to determine the applicability of the relevant statute of limitations.
- 45 6. AT&T has waived any applicable statute of limitations by stipulation in comments dated August 29, 2006.
- 46 7. Any applicable statute of limitations is tolled as to Verizon from no later than August 30, 2006, because on or before that date Verizon knew the nature of the claim sufficiently to preserve its defense and asserted the Commission should not and could not proceed to assert its jurisdiction until federal legal issues are resolved.

ORDER

- 47 Based on the foregoing discussion and conclusions of law, the Commission enters the following order:
- 48 1. The Secretary is directed to open an investigation docket in this matter.
- 49 2. The Secretary shall issue an administrative order to each telecommunications company offering Washington intrastate wireline telecommunications services directing the company to:
- 50 a. Preserve all records and information, if any exist, about any request by or on behalf of the federal government to provide CPNI and any records or information provided in response, until further order of the Commission, and;
- 51 b. Retain the name of any current or former company official or employee who has personal knowledge of any request by or on behalf of the federal government to provide CPNI and any records or information provided in response, the nature of that person's knowledge, and the last known contact information for that person.

- 52 c. The order shall make clear the nature of the allegations, and that each
 telecommunications company should assume, for purposes of notice and
 information retention purposes, that the allegations may apply to them.
- 53 3. The provisions of CPNI subject to this order are those associated with Washington
 intrastate telecommunications. The carriers subject to this order are
 telecommunications companies providing intrastate wireline service in Washington.
- 54 The Commission retains jurisdiction in this matter to effectuate this Order.

DATED this 27th day of September, 2006.

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION

MARK H. SIDRAN, Chairman

PATRICK J. OSHIE, Commissioner

PHILIP B. JONES, Commissioner

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,)	
)	CIVIL ACTION NO.:
Plaintiff,)	
)	COMPLAINT
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.)	

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 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

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

DATED: Trenton, New Jersey
 June 14, 2006



Assistant Attorney General

Washington, D.C. 20530

June 14, 2006

VIA FACSIMILE AND EMAIL

Bradford A. Berenson, Esq.
Sidley Austin LLP
1501 K Street, NW
Washington, D.C. 20005

John G. Kester, Esq.
Williams & Connolly LLP
725 Twelfth Street, NW
Washington, D.C. 20005

John A. Rogovin, Esq.
Wilmer Hale
1875 Pennsylvania Avenue, NW
Washington, D.C. 20006

Christine A. Varney, Esq.
Hogan & Hartson LLP
555 Thirteenth Street, NW
Washington, D.C. 20004

**Re: Subpoenas Duces Tecum Served on Telecommunications Carriers
Seeking Information Relating to the Alleged Provision of Telephone
Call History Data to the National Security Agency**

Dear Counsel:

This letter is to advise you that today the United States of America has filed a lawsuit against the Attorney General and other officials of the State of New Jersey, as well as AT&T Corp., Verizon Communications, Inc., Qwest Communications International, Inc., Sprint Nextel Corporation, and Cingular Wireless LLC (together the "telecommunications carriers"). That lawsuit seeks a declaration that those state officials do not have the authority to enforce subpoenas duces tecum (hereafter the "subpoenas") recently issued to the telecommunications carriers seeking information relating to the alleged provision of "telephone call history data" to the National Security Agency, and that the telecommunications carriers cannot respond to these subpoenas. A copy of the Complaint the United States has filed, as well as a letter we have sent today to Attorney General Farber, are attached hereto.

As noted in our Complaint and letter to Attorney General Farber concerning those issues, the subpoenas infringe upon federal operations, are contrary to federal law, and are invalid under the Supremacy Clause of the United States Constitution. Responding to the subpoenas – including by disclosing whether or to what extent any responsive materials exist – would violate federal laws and Executive Orders. Moreover, the Director of National Intelligence recently has asserted the state secrets privilege with respect to the very same topics and types of information sought by the subpoenas, thereby underscoring that any such information cannot be disclosed. For these reasons, described in more detail in the attachments hereto, please be advised that we

Messrs. Berenson, Kester, Rogovin, Ms. Varney
Page 2

believe that enforcing compliance with, or responding to, the subpoenas would be inconsistent with and preempted by federal law.

Please do not hesitate to contact Carl Nichols or me should you have any questions in this regard.

Sincerely,

A handwritten signature in black ink, appearing to read 'PK' followed by a stylized flourish.

Peter D. Keisler
Assistant Attorney General

Attachments



Assistant Attorney General

Washington, D.C. 20530

June 14, 2006

VIA FACSIMILE AND FEDERAL EXPRESS

The Honorable Zulima V. Farber
Attorney General of New Jersey
25 Market Street
Trenton, New Jersey 08625

**Re: Subpoenas Duces Tecum Served on Telecommunications Carriers
Seeking Information Relating to the Alleged Provision of Telephone
Call History Data to the National Security Agency**

Dear Attorney General Farber:

Please find attached the Complaint filed today by the United States in the United States District Court for the District of New Jersey, in connection with the subpoenas that you have served on various telecommunications companies (the "carriers") seeking information relating to those companies' alleged provision of "telephone call history data" to the National Security Agency ("NSA"). As set forth in the Complaint, it is our belief that compliance with the subpoenas would place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without harming national security, and that enforcing compliance with these subpoenas would be inconsistent with, and preempted by, federal law.

The subpoenas infringe upon federal operations, are contrary to federal law, and accordingly are invalid under the Supremacy Clause of the United States Constitution for several reasons. The subpoenas seek to compel the disclosure of information regarding the Nation's foreign-intelligence gathering, but foreign-intelligence gathering is an exclusively federal function. Responding to the subpoenas, including disclosing whether or to what extent any responsive materials exist, would violate various specific provisions of federal statutes and Executive Orders. And the recent assertion of the state secrets privilege by the Director of National Intelligence in cases regarding the very same topics and types of information sought by your subpoenas underscores that any such information cannot be disclosed.

Although we have filed the attached Complaint at this juncture in light of the return date on the subpoenas (June 15), we nevertheless hope that this matter may be resolved amicably, and

that litigation will prove unnecessary. Toward that end, this letter outlines the basic reasons why, in our view, the state-law subpoenas are preempted by federal law. We sincerely hope that, in light of governing law and the national security concerns implicated by the subpoenas, you will withdraw them, thereby avoiding needless litigation. The United States very much appreciates your consideration of this matter.

1. There can be no question that the subpoenas 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*, 4 U.S. 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).

The subpoenas demand that each carrier produce information regarding specified categories of communications between that carrier and the NSA since September 11, 2001, including "[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 any and all Executive Orders, court orders, or warrants "provided to [the carrier] concerning any demand or request to provide Telephone Call History Data to the NSA"; "[a]ll Documents concerning the basis for [the carrier's] provision of Telephone Call History Data to the NSA, including, but not limited to, any legal or contractual authority"; and "[a]ll Documents concerning any written or oral contracts, memoranda of understanding, memoranda of agreement, other agreements or correspondence by or on behalf of [the carrier] and the NSA concerning the provision of Telephone Call History Data to the NSA." *See* Document Requests, ¶¶ 1-13. In seeking to exert regulatory authority² with respect to the nation's foreign-intelligence gathering, you have thus sought to use your state regulatory authority to intrude upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with federal

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

² The subpoenas make clear 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."

prerogatives. That effort is fundamentally inconsistent with the Supremacy Clause. *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316, 326-27, 4 L.Ed. 579 (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 these state-law subpoenas 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, the subpoenas 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; those subpoenas, just like the subpoenas at issue in *Garamendi*, 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. Responding to the subpoenas, including merely disclosing whether or to what extent any responsive materials exist, would violate various federal statutes and Executive Orders. 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.*³ (As set forth below, the DNI has determined that disclosure of the types of information sought by the subpoenas would harm national security.) Similarly, 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

³ 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.

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.” *Ibid.*⁴

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 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).

It also 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).

New Jersey state officials have not 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 your subpoenas seek to compel disclosure of such information to state officials, responding to them would obviously violate federal law.

⁴ 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).

3. The recent assertion of the state secrets privilege by the Director of National Intelligence (“DNI”) in cases regarding the very same topics and types of information sought by your subpoenas underscores that compliance with those subpoenas would be improper. It is well-established that intelligence information relating to the national security of the United States is subject to the Federal Government’s state secrets privilege. *See United States v. Reynolds*, 345 U.S. 1 (1953). The privilege encompasses a range of matters, including information the disclosure of which would result in an “impairment of the nation’s defense capabilities, disclosure of intelligence-gathering methods or capabilities, and disruption of diplomatic relations with foreign Governments.” *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983), *cert. denied sub nom. Russo v. Mitchell*, 465 U.S. 1038 (1984) (footnotes omitted); *see also Halkin v. Helms*, 690 F.2d 977, 990 (D.C. Cir. 1982) (state secrets privilege protects intelligence sources and methods involved in NSA surveillance).

In ongoing litigation in the United States District Court for the Northern District of California, the DNI has formally asserted the state secrets privilege regarding the very same topics and types of information sought by your subpoenas. *See Hepting v. AT&T Corp.*, No. 06-0672-VRW (N.D. Cal.). In particular, the DNI’s assertion of the privilege encompasses “allegations about NSA’s purported involvement with AT&T,” Negroponte Decl. ¶12, because “[t]he United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets.” *Id.* ¶ 12. As DNI Negroponte has explained, “[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 also* Alexander Decl. ¶8. As DNI Negroponte has further explained, to disclose further details about the intelligence activities of the United States “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. Those concerns are particularly acute when we are facing the threat of terrorist attacks on United States soil.

In seeking information bearing upon NSA’s purported involvement with various telecommunications carriers, your subpoenas 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 the subpoenas are 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 Director of National Intelligence. Any application of state law that would compel such disclosures notwithstanding the DNI’s assessment would contravene

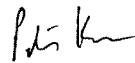
the DNI's authority and the Act of Congress conferring that authority. More broadly, the subpoenas involve an improper effort to use state law to regulate or oversee federal functions, and implicate federal immunity under the Supremacy Clause.

* * *

For the reasons outlined above, the United States believes that the subpoenas and the application of state law they embody are plainly inconsistent with and preempted under the Supremacy Clause, and that compliance with the subpoenas would place the carriers 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. In this light, we sincerely hope that you will withdraw the subpoenas, 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

cc: Bradford A. Berenson, Esq.
John G. Kester, Esq.
John A. Rogovin, Esq.
Christine A. Varney, Esq.

Attachments

UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

THE UNITED STATES OF AMERICA,)	
)	CIVIL ACTION NO.:
Plaintiff,)	
)	COMPLAINT
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.)	

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
DISTRICT OF CONNECTICUT

THE UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	CIVIL ACTION NO.:
)	
v.)	COMPLAINT
)	
ANTHONY J. PALERMINO, in his official)	
capacity as Commissioner of the Connecticut)	
Department of Public Utility Control; DONALD)	
W. DOWNES, in his official capacity as)	
Chairman of the Connecticut Department of Public)	
Utility Control; JACK R. GOLDBERG, in his)	
official capacity as Vice-Chairman of the)	
Connecticut Department of Public Utility Control;)	
JOHN W. BETKOSKI, III, in his official)	
capacity as Commissioner of the Connecticut)	
Department of Public Utility Control; ANNE C.)	
GEORGE, in her official capacity as)	
Commissioner of the Connecticut Department)	
of Public Utility Control; AT&T, CORP.;)	
SOUTHERN NEW ENGLAND)	
TELECOMMUNICATIONS CORP. d/b/a)	
AT&T CONNECTICUT; THE WOODBURY)	
TELEPHONE CO. d/b/a AT&T WOODBURY;)	
VERIZON NEW YORK, INC.)	
)	
Defendants.)	

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 Connecticut Department of Public Utility Control ("DPUC") have sought to obtain, and require the production of, from

telecommunications carriers without proper authorization from the United States. Compliance with the order, issued by those officers, compelling responses to interrogatories 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 order would require disclosure of the details of that activity. The defendant state officers' attempts to order the disclosure of 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, and enter an injunction to the effect that, the State Defendants do not have the authority to seek confidential and sensitive federal government information and thus cannot enforce the order 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 Connecticut 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 Anthony J. Palermino is a Commissioner of the Connecticut Department of Public Utility Control, which maintains its offices in New Britain, Connecticut in Hartford County. He is being sued in his official capacity.
6. Defendant Donald W. Downes is the Chairman of the Connecticut Department of Public Utility Control, which maintains its offices in New Britain, Connecticut in Hartford County. He is being sued in his official capacity.

7. Defendant Jack R. Goldberg is the Vice-Chairman of the Connecticut Department of Public Utility Control, which maintains its offices in New Britain, Connecticut in Hartford County. He is being sued in his official capacity.

8. Defendant John W. Betkoski, III is a Commissioner of the Connecticut Department of Public Utility Control, which maintains its offices in New Britain, Connecticut in Hartford County. He is being sued in his official capacity.

9. Defendant Anne C. George is a Commissioner of the Connecticut Department of Public Utility Control, which maintains its offices in New Britain, Connecticut in Hartford County. She is being sued in his official capacity.

10. Defendant AT&T Corporation is a corporation incorporated in the state of New York, with principle place of business in New Jersey, and that has received a copy of the order requiring responses to the interrogatories in question.

11. Defendant The Southern New England Telephone Company d/b/a AT&T Connecticut is a corporation incorporated in the state of Connecticut, with principle place of business in Connecticut, and that has received a copy of the order requiring responses to the interrogatories in question.

12. Defendant The Woodbury Telephone Company d/b/a AT&T Woodbury is a corporation incorporated in the state of Connecticut with principle place of business in Connecticut, and that has received a copy of the order requiring responses to the interrogatories in question.

13. Defendant Verizon New York Inc. is a corporation incorporated in the state of New York with a principle place of business in New York, and that has received a copy of the order requiring responses to the interrogatories in question.

14. Defendants Palermino, Downes, Goldberg, Betkoski, and George are referred to as the “State Defendants.”

15. Defendants AT&T Inc., SBC Communications d/b/a Southern New England Telecommunications Corp., Woodbury Telephone Co., and Verizon New York, 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.

16. 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.

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

18. 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.”

19. 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.

20. 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.

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

22. 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).

23. 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).

24. 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.

25. 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

26. 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 some of the Carrier Defendants in this case. 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).

27. Since January 2006, more than 30 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. An example of the second kind of case is *Terkel v. AT&T, et al.*, filed in the Northern District of Illinois in May 2006. Case No. C-06-2837 (MFK).

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

30. In both the *Hepting* and *Terkel* 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.

31. As was the case in *Terkel*, where the United States invoked the state secrets privilege, the Order at issue here seek information in an attempt to confirm or deny the existence of this alleged program subject to the USA Today article.

32. In *Terkel*, Director Negroponte concluded 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.

33. 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 the precise subject matter sought from the Carrier Defendants here.

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

34. The DPUC proceeding began on May 24, 2006, when a complaint was filed by American Civil Liberties Union of Connecticut (“ACLU-CT”) requesting that the DPUC open an investigation into whether AT&T and Verizon, in Connecticut, were aiding the NSA by allegedly providing customer information to the NSA. The Carrier Defendants subject to the complaint 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.

35. On August 10, 2006, the ACLU-CT issued interrogatories to the Carrier Defendants that, among other things, seeks to “require that Verizon provide sworn affirmations of representations it made in its filed response to the complaint.” Representative copies of the August 10, 2006 interrogatories to AT&T and Verizon are attached as Exhibit C. The interrogatories unquestionably seek to require the Carrier Defendants to provide information regarding the allegations that the Carrier Defendants aided in alleged foreign intelligence gathering operations as reported in the media. Thus, the interrogatories seek to compel information regarding, *inter alia*, whether the Carrier Defendant “disclosed customer information and/or records to private parties, government entities¹ and/or law enforcement personnel when

¹ Government entity refers to and “includes any entity or person operating as part of the collective government of the United States of America, federal as well as state, including but not limited to the Department of Homeland Security, the Department of Emergency Management and Homeland Security, the Federal Bureau of Investigation, the National Security Agency, the Central Intelligence Agency and/or any branch of the United States Armed Forces, their present

not compelled to do so by subpoena, warrant, court order or a request under 18 U.S.C. § 2709 ("National Security Letter" or "NSL"); the "full details of each occasion on which AT&T disclosed customer information and/or records to private parties, government entities and/or law enforcement personnel when not compelled to do so by subpoena, warrant, court order or NSL, including the date of each request, the information sought, the information provided, and the date on which the information was provided"; and whether "AT&T had any policy or policies during the Relevant Period, whether written or unwritten, concerning the disclosure of customer information and/or records to private parties, government entities and/or law enforcement personnel when not compelled to do so by subpoena, warrant, court order or NSL." Exh. C at 4.

36. On August 23, 2006, the DPUC issued an order (the "Order") requiring the Carrier Defendants to respond to these interrogatories, a copy of the Order is attached at Exhibit D. The DPUC's Order "determined that the ACLU-CT should be allowed the opportunity to conduct discovery in support of its claims." In so doing, the DPUC specifically denied the Carrier Defendants' motion to strike these interrogatories. The Order demands that "[i]nterrogatory responses should be filed no later than September 7, 2006." Exhibit D at 2.

37. 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).

or former personnel, agents or employees and/or any entity or person working under the direction, influence or control of such persons or entities." Exh. C at 2.

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

38. The State Defendants' attempts to seek, require disclosure of, or otherwise obtain the information requested by the August 23, 2006 Order and interrogatories, as well as any related information, is fundamentally inconsistent with and their authority is preempted by the Federal Government's exclusive control over all foreign intelligence gathering activities under the Constitution and federal statute. 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 ordered responses to the interrogatories seek to force 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.

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 interrogatories.

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 Order.

45. The very attempt by the State Defendants to investigate the alleged foreign intelligence gathering activities of the United States constitutes a continuing injury to the sovereign interests of the United States as the states are without authority under the U.S. Constitution to regulate or obstruct the operations of the Federal Government.

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

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

47. 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.

48. 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 Connecticut Department of Public Utility Control, 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)**

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

50. Providing responses to the Order 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 Order issued by the State Defendants, or other similar order, 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 this Order 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: September 6, 2006

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

KEVIN J O'CONNOR
United States Attorney

CARL J. NICHOLS

Deputy Assistant Attorney General

DOUGLAS LETTER
Terrorism Litigation Counsel

ARTHUR R. GOLDBERG
Assistant Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Special Litigation Counsel

ALEXANDER K. HAAS (CA Bar 220932)
Trial Attorney, Federal Programs Branch
United States Department of Justice
P.O. BOX 883
WASHINGTON, DC 20044
(202) 307-3937

_____/s/_____
WILLIAM A. COLLIER (ct00986)
Assistant United States Attorney
U.S. Attorney's Office
450 Main Street, Room 328
Hartford, CT 06103
Tel.: (860) 947-1101
Fax: (860) 240-3291
william.collier@usdoj.gov

Exhibit 14
Page 1 of 16

UNITED STATES DISTRICT COURT
DISTRICT OF VERMONT

U.S. DISTRICT COURT
DISTRICT OF VERMONT
FILED

2006 OCT -2 PM 3:49

THE UNITED STATES OF AMERICA,

Plaintiff,

v.

JAMES VOLZ, in his official capacity as
Chairman of the Vermont Public Service Board;
DAVID C. COEN in his official capacity as
Board Member of the Vermont Public Service
Board; JOHN D. BURKE in his official capacity as
Board Member of the Vermont Public Service
Board; DAVID O'BRIEN, in his official capacity
as Commissioner of the Vermont Department of
Public Service; AT&T COMMUNICATIONS OF
NEW ENGLAND, INC.; and VERIZON NEW
ENGLAND INC. D/B/A VERIZON VERMONT,

Defendants.

CIVIL ACTION NO.:

COMPLAINT 2:06-cv-188

CLERK

BY

DEPUTY CLERK

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 Vermont Public Service
Board ("VPSB") and Vermont Department of Public Service ("VDPS") have sought to obtain
from telecommunications carriers without proper authorization from the United States.

Compliance with the ordered production or similar discovery, issued by those officers under state
law, 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

Exhibit 14
Page 2 of 16

national security. And if particular carriers are indeed supplying foreign intelligence information to the Federal Government, compliance with the order would require disclosure of the details of that activity. The defendant state officers' attempts to order the disclosure of 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. The VPSB and VDPS have no authority to investigate the alleged foreign-intelligence gathering functions of the United States. This Court should therefore enter a declaratory judgment that the defendant state officers do not have the authority to require the disclosure of confidential and sensitive federal government information and thus cannot enforce the order they have served on the telecommunications carriers to the extent it seeks information related to the alleged federal operations of the United States, and should enter an injunction prohibiting such actions.

JURISDICTION AND VENUE

2. The Court has jurisdiction pursuant to 28 U.S.C. §§ 1331, 1345.
3. Venue lies in the District of Vermont 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 James Volz is the Chairman of the Vermont Public Service Board, which maintains its offices in Montpelier, Vermont in Washington County. He is being sued in his official capacity.
6. Defendant David C. Coen is a Board Member of the Vermont Public Service Board, which maintains its offices in Montpelier, Vermont in Washington County. He is being sued in his official capacity.
7. Defendant John D. Burke is a Board Member of the Vermont Public Service Board,

Exhibit 14
Page 3 of 16

which maintains its offices in Montpelier, Vermont in Washington County. He is being sued in his official capacity.

8. Defendant David O'Brien is the Commissioner of the Vermont Department of Public Service, which maintains its offices in Montpelier, Vermont in Washington County. He is being sued in his official capacity.

9. Defendant AT&T Communications of New England, Inc., is a New York corporation with its principal place of business in New Jersey and operates in the State of Vermont. It is a wholly owned subsidiary of AT&T Corporation, and has received a copy of the order requiring responses to information requests of a Vermont agency.

10. Defendant Verizon New England Inc. d/b/a Verizon Vermont is a New York corporation with a principal place of business in Boston, Massachusetts and operates in the State of Vermont and has received a copy of the order requiring responses to information requests of a Vermont agency.

11. Defendants Volz, Coen, Burke, and O'Brien are referred to as the "State Defendants."

12. Defendants AT&T Communications of New England, Inc., and Verizon New England Inc. d/b/a Verizon Vermont 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.

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

Exhibit 14
Page 4 of 16

the performance of the country's national security function.

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

15. 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."

16. 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.

17. 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.

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

19. 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

Exhibit 14
Page 5 of 16

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).

20. 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).

21. 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.

22. 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."

Exhibit 14
Page 6 of 16

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

23. 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 some of the Carrier Defendants in this case. No United States official has confirmed or denied the existence of the alleged program subject of 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).

24. Since January 2006, more than 30 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.

25. 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. An example of the second kind of case is *Terkel v. AT&T, et al.*, filed in the Northern District of Illinois in May 2006. Case No. C-06-2837 (MFK).

26. On August 9, 2006, the Judicial Panel on Multidistrict Litigation granted a motion to transfer all of these lawsuits to a single district court – the U.S. District Court for the Northern District of California – for pretrial proceedings. *In re: National Security Agency Telecommunications Records Litigation*, MDL Docket No. 1791 (JPML).

Exhibit 14
Page 7 of 16

27. In both the *Hepting* and *Terkel* 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.

28. As was the case in *Terkel*, where the United States invoked the state secrets privilege, the Order at issue here seeks information in an attempt to confirm or deny the existence of this alleged program subject to the USA Today article.

29. In *Terkel*, Director Negroponte concluded 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

Exhibit 14
Page 8 of 16

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.

30. 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 the precise subject matter sought from the Carrier Defendants here.

31. Every court to rule on the telephone records issue has upheld that privilege assertion. See *Terkel v. AT&T Corp.*, 2006 WL 2088202, at *17 (N.D. Ill. July 25, 2006) (dismissing case on state secrets grounds because “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 . . . [and] therefore adversely affect our national security”); *ACLU v. NSA*, 438 F. Supp. 2d 754, 765 (E.D. Mich. 2006) (dismissing, on state secrets grounds, “data-mining” claims regarding alleged NSA activities); *Hepting v. AT&T Corp.*, No C-06-672, 2006 WL 2038464 (N.D. Cal. July 20, 2006) (declining to

Exhibit 14
Page 9 of 16

permit any discovery into allegations about AT&T's involvement in an alleged communication records program).

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

32. The State of Vermont began its attempts to investigate the alleged foreign-intelligence gathering functions of the United States in response to the USA Today article mentioned above, *see* ¶ 22, *supra*. Less than a week after that article appeared, on May 17, 2006, the VDPS sent information requests to one of the Carrier Defendants “[p]ursuant to its statutory authority under 30 V.S.A. § 206” requiring responses to a variety of questions pertaining to the alleged relationship between that Carrier Defendant and the NSA. *See* Letter from Commissioner David O’Brien to Jay E. Gruber, 1-3 (May 17, 2006), a copy of which is attached hereto as Exhibit C.

33. On June 21, 2006, the VDPS petitioned the VPSB to open an “Investigation into Alleged Unlawful Customer Records Disclosed by AT&T Communications of New England, Inc.” *See* Letter from Special Counsel Leslie A. Cadwell to Susan M. Hudson, 1 (June 21, 2006), attached hereto (with enclosures) at Exhibit D. The VDPS petition makes clear that the purpose of the investigation is to use state regulatory power to obtain “information from AT&T regarding the alleged disclosure of customer information to the National Security Agency and any other state or federal agency.” *See* Exh. D at p. 2, ¶ 2; *see also id.* ¶¶ 3-6.

34. On June 29, 2006, the VPSB issued an order opening an investigation based on the VDPS complaint. *See* June 29, 2006 Procedural Order of the VPSB, attached as Exhibit E. The Carrier Defendants filed motions to dismiss these proceedings, arguing that the federal law preempted the state law underlying the authority of the VPSB.

Exhibit 14
Page 10 of 16

35. The VPSB itself originally recognized that federal law limits its authority to seek information regarding alleged intelligence-gathering activities. The VPSB issued a Procedural Order on July 12, 2006, that observed there may be “incompatible state and federal obligations” on the carriers and expressed an interest in avoiding an imposition of such obligations. *See* July 12, 2006 Procedural Order of the VPSB at 3, attached hereto as Exhibit F. This Order also inquired of the United States’ views. The United States Department of Justice subsequently advised the VPSB by letter 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 VPSB that any authority to obtain information regarding the foreign-intelligence gathering functions of the United States in this instance is impermissible under the U.S. Constitution and otherwise preempted by federal law. *See* Letter from Peter D. Keisler to the VPSB (July 28, 2006), attached as Exhibit G (without enclosures). This letter did not constitute an intervention by the United States or constitute an acceptance of state authority over the United States. *Id.* at 1.

36. On September 18, 2006, the VPSB denied the motions to dismiss these proceedings concluding that federal law did not preempt its authority. *See* September 18, 2006 Procedural Order of the VPSB, attached as Exhibit H. The VPSB also authorized discovery against the Carrier Defendants.

37. On September 21, 2006, the VPSB issued an order that AT&T “shall provide an additional response to the information request from the Vermont Department of Public Service issued on May 17, 2006, under the authority of 30 V.S.A. § 206.” *See* September 21, 2006 Procedural Order of the VPSB at 1 (the “Order”), attached as Exhibit I. The Order purports to require responses by October 2, 2006. The information requests, *see* Exhibit C hereto, expressly

Exhibit 14
Page 11 of 16

seek to investigate the alleged foreign intelligence surveillance activities of the Federal Government, specifically by seeking information about the carriers alleged involvement with the NSA or other federal agencies. The Order therefore purports to require, among other things, the carrier to: state whether it “disclosed or delivered to the National Security Agency (“NSA”) the phone call records of any AT&T customers in Vermont at any time since January 1, 2001” and that “if any such disclosures occurred prior to the date specified, please provide the date on which the disclosures commenced”; “identify the categories of information AT&T provided to the NSA, including the called and calling parties' numbers; date of call; time of call; length of call, name of called and calling parties; and the called and calling parties' addresses”; state whether it “disclosed or delivered to any other state or federal agency the phone call records of any AT&T customer in Vermont since January 1, 2001”; “describe the format in which the information was provided (e.g. database with information on a call-by-call basis)”; “describe the reporting interval for the provision of such information (e.g. monthly, annually etc.)”; “[s]tate whether the disclosures of [] Vermont customer call information to the NSA and/or any state or federal agency is ongoing” and the “number of occasions” the alleged disclosures occurred; state whether it is “disclosing records for any communications services other than telephone calling records (e.g. records for e-mail or internet access)”; state “whether any such disclosures were made . . . voluntarily upon request of a governmental agency” or “in response to an exercise of governmental authority”; and to describe whether the carrier “modified any of its equipment or other physical plant in Vermont to permit access to data and other information carried on its network by any agency of the federal government” and “the location, equipment, and details of such modifications, and state the purpose for permitting such access.” *See* Exh. C at ¶¶ 1-16.

38. A comprehensive body of federal law governs the field of foreign intelligence

Exhibit 14
Page 12 of 16

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.

39. The State Defendants' attempts to seek, require disclosure of, or otherwise obtain the information requested by the September 21, 2006 Order incorporating the May 17, 2006 information requests, as well as any related information sought in the contemplated discovery against all Carrier Defendants, are fundamentally inconsistent with and are preempted by the Federal Government's exclusive control over all foreign intelligence gathering activities under the Constitution and federal statute. In addition, no federal law authorizes the State Defendants to obtain the information they seek.

40. 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.

41. 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.

42. In seeking information bearing upon NSA's purported involvement with the Carrier Defendants, the State Defendants seek to force 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

Exhibit 14
Page 13 of 16

intelligence sources and methods.

43. 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.

44. 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 Order to the extent it seeks to investigate alleged federal operations.

45. 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 Order.

46. The very attempt by the State Defendants to investigate the alleged foreign intelligence gathering activities of the United States constitutes a continuing injury to the sovereign interests of the United States as the states are without authority under the U.S. Constitution to regulate or obstruct the operations of the Federal Government.

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

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

48. 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

Exhibit 14
Page 14 of 16

exclusive control over foreign intelligence gathering activities, national security, the conduct of foreign affairs, and the conduct of military affairs.

49. 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 no organ of State government, such as the Vermont Public Service Board or the Vermont, 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)**

50. Plaintiff incorporates by reference paragraphs 1 through 49 above.

51. Providing responses to the Order 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 Order issued by the State Defendants, or other similar order or request for discovery, 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 this Order to the extent it seeks information related to the alleged foreign intelligence gathering operations of the United States 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.

Exhibit 14
Page 15 of 16

2. That this Court enter a declaratory judgment pursuant to 28 U.S.C. § 2201(a), that the State Defendants lack the authority to investigate the alleged foreign intelligence gathering activities of the United States, and specifically the alleged involvement, or lack thereof, of the Carrier Defendants in the alleged activities, because of the Federal Government's exclusive control under the U.S. Constitution over foreign intelligence gathering activities, national security, the conduct of foreign affairs, and the conduct of military affairs.

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

Dated: October 2, 2006

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

THOMAS D. ANDERSON
United States Attorney

CARL J. NICHOLS
Deputy Assistant Attorney General

DOUGLAS LETTER
Terrorism Litigation Counsel

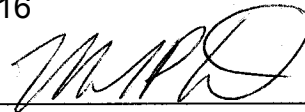
ARTHUR R. GOLDBERG
Assistant Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Special Litigation Counsel


ALEXANDER K. HAAS

Pro hac vice application pending
Trial Attorney, Federal Programs Branch
United States Department of Justice
P.O. Box 883
Washington, DC 20044
(202) 307-3937

Exhibit 14
Page 16 of 16

A handwritten signature in black ink, appearing to read 'MPD', is written over a horizontal line.

MICHAEL P. DRESCHER
Assistant United States Attorney
P.O. Box 570
Burlington, VT 05402
(802) 951-6725

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

THE UNITED STATES OF AMERICA,)	
)	CIVIL ACTION NO.:
Plaintiff,)	
)	COMPLAINT
v.)	
)	
STEVE GAW, in his official capacity as)	
Commissioner of the Missouri Public Service)	
Commission; ROBERT M. CLAYTON, III,)	
in his official capacity as Commissioner of the)	
Missouri Public Service Commission;)	
SOUTHWESTERN BELL TELEPHONE, L.P.;)	
SBC ADVANCED SOLUTION, INC.; SBC)	
LONG DISTANCE, LLC; AT&T)	
COMMUNICATIONS OF THE SOUTHWEST,)	
INC.; TCG ST. LOUIS HOLDINGS, INC.; TCG)	
KANSAS CITY, INC.)	
)	
Defendants.)	

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 Missouri Public Service Commission 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 Eastern District of Missouri pursuant to 28 U.S.C. § 1391(b)(1)-(2).

This action properly lies in the Eastern Division of this District. LCvR 3-2.07(A)(1) & (B)(2).

PARTIES

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

5. Defendant Steve Gaw is a Commissioner on the Missouri Public Service Commission, and maintains his offices in Cole County. He is being sued in his official capacity.

6. Defendant Robert M. Clayton, III is a Commissioner on the Missouri Public Service Commission, and maintains his offices in Cole County. He is being sued in his official capacity.

7. Defendant Southwestern Bell Telephone, L.P. is a corporation incorporated in the state of Texas with its principal place of business in Texas that has offices in the City of St. Louis, Missouri and that has received a subpoena in Missouri.

8. Defendant SBC Advanced Solutions, Inc. is a corporation incorporated in the state of Delaware with its principal place of business in the state of Texas, that has offices in St. Louis County, Missouri, and that has received a subpoena in Missouri.

9. Defendant SBC Long Distance, LLC is a corporation incorporated in the state of Delaware with its principal place of business in the state of California, that has received a subpoena in Missouri.

10. Defendant AT&T Communications of the Southwest, Inc. is a corporation incorporated in the state of Delaware with its principal place of business in the state of New Jersey, that has offices in St. Louis County, Missouri, and that has received a subpoena in Missouri.

11. Defendant TCG St. Louis Holdings, Inc. is a corporation incorporated in the state of Missouri with its principal place of business in the state of New Jersey that has offices in St. County, Missouri, and that has received a subpoena in Missouri.

12. Defendant TCG Kansas City, Inc. is a corporation incorporated in the state of Delaware with its principal place of business in the state of New Jersey, that has no offices Missouri, and that has received a subpoena in Missouri.¹

13. Defendants Southwestern Bell Telephone, L.P., SBC Advanced Solutions, Inc., SBC Long Distance, LLC, AT&T Communications of the Southwest, Inc., TCG St. Louis Holdings, Inc., and TCG Kansas City, 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-

¹ Defendants Gaw and Clayton have not sought enforcement of the subpoenas with respect to TCG Kansas City, Inc., so the paragraphs below discussing enforcement deal solely with the other Carrier Defendants.

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

24. 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 three of the Carrier Defendants in this case. 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 (“Alexander Decl.”) ¶ 8 (Exhibit A, attached to this Complaint).

25. Since January 2006, more than 30 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.

26. 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. An example of the second kind of case is *Terkel v. AT&T, et al.*, filed in the Northern District of Illinois in May 2006. Case No. C-06-2837 (MFK).

27. 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).

28. In both the *Hepting* and *Terkel* 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.

29. As was the case in *Terkel*, where the United States invoked the state secrets privilege, the subpoenas at issue here seek information in an attempt to confirm or deny the existence of this alleged program subject to the USA Today article.

30. In *Terkel*, Director Negroponte concluded 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.

31. 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 the precise subject matter sought from the Carrier Defendants here.

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

32. On June 19, 2006, and June 22, 2006, the State Defendants sent subpoenas ad testificandum and subpoenas duces tecum, respectively (“Subpoenas”) to each of the Carrier Defendants. Representative copies of these subpoenas ad testificandum and subpoenas duces tecum are attached as Exhibits C and D. The testimony sought by the subpoenas ad testificandum related to, “[t]he number of Missouri customers, if any, whose calling records have been delivered or otherwise disclosed to the National Security Agency (“NSA”) and whether or

not any of those customers were notified that their records would be or had been so disclosed and whether or not any of those customers consented to the disclosure;” “[t]he legal authority, if any, under which the disclosures . . . were made;” “[t]he nature or type of information disclosed to the NSA, including telephone number, subscriber name and address, social security numbers, calling patterns, calling history, billing information, credit card information, internet data, and the like;” “[t]he date or dates on which the disclosures . . . were made;” and “[t]he particular exchanges for which any number was disclosed to the NSA.” *See* Exhibit C, subpoena ad testificandum, attachment A ¶¶ 1-5. In turn, the materials sought by the subpoenas duces tecum include, among other items, “[a]ny order, subpoena or directive of any court, tribunal or administrative agency or officer whatsoever, directing or demanding the release of customer proprietary information relating to Missouri customers;” and “[c]opies of all records maintained pursuant to PSC Rule 4 CSR 240-33.160(6) involving the disclosure of CPNI to a third party.” *See* Exhibit D, subpoena duces tecum, attachment A, ¶¶ 1-4.

33. These Subpoenas specify that they are issued “pursuant to Sections 386.130, 386.320, 386.410, 386.420, 386.440, 386.460, and 386.480, RSMo.” The cited provisions of state law provide, *inter alia*, that “commission shall have the general supervision of all telegraph corporations or telephone corporations, and telegraph and telephone lines . . . and shall have power to and shall examine the same and keep informed as to their general condition, their capitalization, their franchises and the manner in which their lines and property, owned, leased, controlled or operated are managed, conducted and operated, not only with respect to the adequacy, security and accommodation afforded by their service, but also with respect to their compliance with all the provisions of law, orders and decisions of the commission and charter and franchise requirements. RSMo. 386.320 ¶1. Furthermore, the “commission and each

commissioner shall have power to examine all books, contracts, records, documents and papers of any person or corporation subject to its supervision, and by subpoena duces tecum to compel production thereof. *Id.* ¶ 3. These provisions also provide that, “[t]he commission or any commissioner or any party may, in any investigation or hearing before the commission, cause the deposition of witnesses . . . and to that end may compel the attendance of witnesses and the production of books, waybills, documents, papers, memoranda and accounts.” RSMo. 386.420 ¶ 2.

34. These Subpoenas demanded that responses be submitted by the Carrier Defendants on or before July 12, 2006. On July 11, 2006, the General Counsel for the Office of the Director of National Intelligence, Benjamin A. Powell, advised the Carrier Defendants that compliance with these subpoenas could not be accomplished without harming national security and further advised that enforcement of the subpoenas would be inconsistent with federal law. *See* Letter of July 11, 2006, from Benjamin A. Powell to Edward R. McNicholas, attached as Exhibit E. Indeed, a comprehensive body of federal law governs the field of foreign intelligence gathering and bars any unauthorized disclosures as contemplated by these subpoenas, 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).

35. The State Defendants initiated proceedings in the Circuit Court for the County of Cole on July 12, 2006 to seek to compel the Carrier Defendants to comply.

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

36. 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.

37. 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.

38. 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.

39. In seeking information bearing upon NSA's purported involvement with the Carrier Defendants, the Subpoenas 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.

40. 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.

41. 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.

42. 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)**

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

44. 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.

45. The Subpoenas, and any responses required thereto, are also invalid because the no organ of State government, such as the Missouri Public Services 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)**

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

47. 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 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.

Dated: July 25, 2006

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General


CATHERINE L. HANAWAY
United States Attorney

CARL J. NICHOLS
Deputy Assistant Attorney General

DOUGLAS LETTER
Terrorism Litigation Counsel

ARTHUR R. GOLDBERG
Assistant Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Special Litigation Counsel


ALEXANDER K. HAAS (CA Bar 220932)
Trial Attorney, Federal Programs Branch
UNITED STATES DEPARTMENT OF
JUSTICE
P.O. BOX 883
WASHINGTON, DC 20044
(202) 307-3937



U. S. Department of Justice

Civil Division

Deputy Assistant Attorney General

Washington, D.C. 20530

August 21, 2006

By First Class Mail and Electronically

John A. Rogovin, Esq.
Samir C. Jain, Esq.
Wilmer Hale
1875 Pennsylvania Avenue, NW
Washington, D.C. 20006

Re: Maine Public Utilities Commission Docket 2006-274

Dear Counsel:

This letter is to advise you that today the United States of America has filed a lawsuit against officials of the State of Maine, as well as Verizon. That lawsuit seeks a declaration that those state officials do not have the authority to require Verizon to provide information to the Maine Public Utilities Commission ("MPUC") regarding any alleged relationship Verizon may or may not have with the National Security Agency. A copy of the Complaint the United States has filed is enclosed hereto.

As set forth in the Complaint, the MPUC's actions infringe upon federal operations, are contrary to federal law, and are invalid under the Supremacy Clause of the United States Constitution. Thus, responding to the State Defendants' requests for information such as the MPUC's August 9, 2006 Order, including by disclosing whether or to what extent any responsive materials exist, would violate federal laws and Executive Orders. Moreover, the Director of National Intelligence has asserted the state secrets privilege with respect to the same kinds of information sought by the MPUC, thereby underscoring that any such information cannot be required by a state entity.

For these reasons, described in more detail in the complaint, please be advised that we believe that enforcing compliance with, or responding to, the MPUC's demands for information would be inconsistent with, and preempted by, federal law.

Jon A. Rogovin, Esq.
Samir C. Jain, Esq.
Page 2

Please do not hesitate to contact me should you have any questions in this regard.

Sincerely,

A handwritten signature in black ink, appearing to read "Carl J. Nichols". The signature is fluid and cursive, with a prominent "C" and "N".

Carl J. Nichols
Deputy Assistant Attorney General

Enclosure

Exhibit 17
Page 1 of 2

JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION

SEP 28 2006

FILED
CLERK'S OFFICE

DOCKET NO. 1791

BEFORE THE JUDICIAL PANEL ON MULTIDISTRICT LITIGATION
IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS
RECORDS LITIGATION

(SEE ATTACHED SCHEDULE)

CONDITIONAL TRANSFER ORDER (CTO-3)

On August 9, 2006, the Panel transferred 15 civil actions to the United States District Court for the Northern District of California for coordinated or consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407. *See* ____ F.Supp.2d ____ (J.P.M.L. 2006). Since that time, 16 additional actions have been transferred to the Northern District of California. With the consent of that court, all such actions have been assigned to the Honorable Vaughn R. Walker.

It appears that the actions on this conditional transfer order involve questions of fact that are common to the actions previously transferred to the Northern District of California and assigned to Judge Walker.

Pursuant to Rule 7.4 of the Rules of Procedure of the Judicial Panel on Multidistrict Litigation, 199 F.R.D. 425, 435-36 (2001), these actions are transferred under 28 U.S.C. § 1407 to the Northern District of California for the reasons stated in the order of August 9, 2006, and, with the consent of that court, assigned to the Honorable Vaughn R. Walker.

This order does not become effective until it is filed in the Office of the Clerk of the United States District Court for the Northern District of California. The transmittal of this order to said Clerk shall be stayed 15 days from the entry thereof. If any party files a notice of opposition with the Clerk of the Panel within this 15-day period, the stay will be continued until further order of the Panel.

FOR THE PANEL:

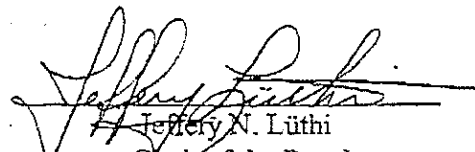

Jeffrey N. Lüthi
Clerk of the Panel

Exhibit 17

Page 2 of 2

SCHEDULE CTO-3 - TAG-ALONG ACTIONS

DOCKET NO. 1791

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS
LITIGATIONDIST. DIV. C.A.#CASE CAPTIONCONNECTICUT
CT 3 06-1405

United States of America v. Anthony J. Palermo, et al.

MAINE
ME 1 06-97

United States of America v. Kurt Adams, et al.

MISSOURI EASTERN
MOE 4 06-1132

United States of America v. Steve Gaw, et al.

MISSOURI WESTERN
MOW 2 06-4177

Robert Clayton, et al. v. AT&T Communications of the Southwest, Inc., et al.

NEW JERSEY
NJ 3 06-2683

United States of America v. Zulima V. Farber, et al.



Assistant Attorney General

Washington, D.C. 20530

September 19, 2006

VIA FACSIMILE AND FEDERAL EXPRESS

Michigan Public Service Commission
Post Office Box 30221
Lansing, Michigan 48909

Attn: Chairman J. Peter Lark
Commissioner Laura Chappelle
Commissioner Monica Martinez

Re: Case No. U-14985 - ACLU v AT&T of Michigan and Verizon

Dear Chairman Lark and Commissioners Chappelle and Martinez:

I write with regard to the above-referenced case pending before Administrative Law Judge Eyster and the Michigan Public Service Commission ("MPSC"). I understand that motions to dismiss these proceedings are currently pending before the MPSC, and the United States of America would like to take the opportunity to provide its views to the MPSC as it considers how to proceed. Please note, however, that our willingness to provide our views is not, and should not be deemed, either a formal intervention in this matter or the submission of the United States to the jurisdiction of the State of Michigan.

The American Civil Liberties Union of Michigan ("ACLU") initiated these proceedings against AT&T of Michigan and Verizon (collectively the "carriers") in July after *USA Today* published an article alleging that the National Security Agency ("NSA") has been secretly collecting the phone call records of millions of Americans from various telecommunications carriers. See Letter of July 26, 2006 from ACLU to MPSC (the "ACLU Letter"), attached hereto (without attachments). In particular, the ACLU requests that a formal investigation be opened so that the MPSC can attempt to ascertain the truth of the allegations in the news reports regarding the purported United States' foreign intelligence gathering program, which the ACLU asserts may have violated Michigan law.

It is the position of the United States that, in light of the allegations on the face of the ACLU Letter, the MPSC lacks any authority to proceed with the investigation in this case and that the only prudent course of action would be to grant the pending motions to dismiss.

Chairman J. Peter Lark
Commissioner Laura Chappelle
Commissioner Monica Martinez
Page 2

Notably, the MPSC would be unable to engage in any discovery propounded in this MPSC proceeding because such demands for information would place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without harming national security. Moreover, any attempt to enforce compliance with such requests for information would be inconsistent with, and preempted by, federal law. This letter outlines the basic reasons why, in our view, the MPSC lacks authority to proceed with this investigation, why any discovery propounded in this proceeding would be preempted by federal law, and why compliance with such requests would violate federal law.

In similar situations in New Jersey, Missouri, Maine, and Connecticut, the United States has acted to protect its sovereign interests by filing lawsuits to preclude the enforcement of state commission orders seeking disclosure of similar information. We sincerely hope that, in light of governing law and the national security concerns implicated by this case, you will grant the motions to dismiss 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 the ACLU Letter and Complaint seek to use Michigan state law, through the MPSC, to investigate the nature of, seek the disclosure of information regarding, and obtain orders and relief relating to the Nation's alleged foreign-intelligence gathering activities, and specifically to inquire into whether the carriers have aided a purported NSA intelligence program, *see* ACLU Letter at 2-4. It has been clear since at least *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316, 4 L.Ed. 579 (1819), that state law may not regulate the Federal Government or obstruct federal operations. Foreign-intelligence gathering is an exclusively federal function; it concerns three overlapping areas that are peculiarly the province of the National Government: (i) foreign relations and the conduct of the Nation's foreign affairs, *see American Insurance Ass'n v. Garamendi*, 539 U.S. 396, 413 (2003); (ii) 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 (iii) 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).

In seeking to exert regulatory authority¹ with respect to the nation's foreign-intelligence gathering, the ACLU asks this body to exercise state regulatory authority to intrude upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with

¹ The ACLU Letter makes clear that the complainants' request is made "pursuant to the jurisdiction and authority granted the MPSC by Sections 201, 202, 203, 205, 213, and 503 of" the state law governing the MPSC. *See* ACLU Letter at 4.

Chairman J. Peter Lark
Commissioner Laura Chappelle
Commissioner Monica Martinez
Page 3

federal prerogatives. That effort is fundamentally inconsistent with the Supremacy Clause. *McCulloch*, 17 U.S. at 326-27 (“[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 proceedings – in particular state-law information requests that would necessarily accompany any investigation – 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. It is clear why this is so. 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”). It is the U.S. Constitution itself that delineates these boundaries, and the organs of state government are incapable of doing what the ACLU asks the MPSC to undertake – investigate alleged foreign-intelligence gathering functions of the United States.

2. If the MPSC does not dismiss this action and goes on to conduct an investigation, it will, through the use of its discovery processes, attempt to require the carriers to respond to the allegations of their alleged involvement with the foreign-intelligence gathering functions of the United States. A response to such demands for information, including merely disclosing whether, or to what extent, any responsive materials exist, would violate various federal statutes and Executive Orders.

First, 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.”² *Ibid.* (emphasis added).

² 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*,

Chairman J. Peter Lark
Commissioner Laura Chappelle
Commissioner Monica Martinez
Page 4

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.*³ (As set forth below, the DNI has determined that disclosure of the types of information sought by the information requests would harm national security.)

In addition, 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 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

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).

³ 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.

Chairman J. Peter Lark
Commissioner Laura Chappelle
Commissioner Monica Martinez
Page 5

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 Michigan state officials nor the ACLU 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 request for information seeks to compel disclosure of such information to state officials or the complainants in this case, responding to those requests would obviously violate federal law.

3. The recent successful assertion of the state secrets privilege by the DNI in *Terkel v. AT&T*, 06-cv-2837 (N.D. Ill.), regarding the very same topics and types of information that are fundamentally at issue in this proceeding, underscores that any further proceedings before the MPSC would be improper. It is well-established that intelligence information relating to the national security of the United States is subject to the Federal Government’s state secrets privilege. See *United States v. Reynolds*, 345 U.S. 1 (1953). The privilege encompasses a range of matters, including information the disclosure of which would result in an “impairment of the nation’s defense capabilities, disclosure of intelligence-gathering methods or capabilities, and disruption of diplomatic relations with foreign Governments.” *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983), cert. denied sub nom. *Russo v. Mitchell*, 465 U.S. 1038 (1984) (footnotes omitted); see also *Halkin v. Helms*, 690 F.2d 977, 990 (D.C. Cir. 1982) (state secrets privilege protects intelligence sources and methods involved in NSA surveillance).

In the *Terkel* case, the DNI has formally, and successfully, asserted the state secrets privilege regarding the very same topics and types of information sought by these requests for information. In particular in *Terkel*, Director Negroponte concluded 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, attached 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.*

Chairman J. Peter Lark
Commissioner Laura Chappelle
Commissioner Monica Martinez
Page 6

In light of the exceptionally grave damage to national security that could result from any such information, Director Negroponte 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.* The assertion of the state secrets privilege in *Terkel* 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. In other words, the state secrets privilege covers the precise subject matter that the ACLU asks Michigan officials to investigate and would cover the discovery process pertaining to these proceedings.

In the *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 v. AT&T Corp.*, 2006 WL 2088202, at *17-19 (N.D. Ill. July 25, 2006). In seeking to have the MPSC exert its investigatory process under Michigan law over the carriers, the MPSC would ask telecommunication carriers to confirm or deny similar information, and thus seek the very type of disclosures deemed inimical to the national security in *Terkel* by both the DNI and Judge Kennelly.⁴ Indeed, in *American Civil Liberties Union v. National Security Agency*, 438 F. Supp. 2d 754, 765-66 (E.D. Mich. Aug. 17, 2006), the Court held that "the state secrets privilege applies to Plaintiffs' data-mining claim" regarding alleged access to call records by the NSA and dismissed that claim. That is precisely the claim that the ACLU asks this body to investigate.

* * *

Accordingly, for the reasons outlined above, it is the United States' position that the MPSC has no authority in this area to investigate the alleged foreign-intelligence gathering

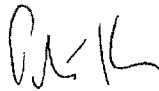
⁴ In another pending case raising similar issues, *Hepting v. AT&T Corp.*, No. 06-0672-VRW (N.D. Cal.), although the Court did not grant the Government's motion to dismiss at this stage, it declined to permit discovery on communications records allegations. The United States respectfully disagrees with the decision not to dismiss the case on state secrets grounds; Judge Walker himself certified his order for immediate appeal, and the United States is seeking such review. 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.

Chairman J. Peter Lark
Commissioner Laura Chappelle
Commissioner Monica Martinez
Page 7

functions of the United States and that the application of state law cited by the ACLU are preempted under the Supremacy Clause. Further, should this action not be dismissed, any request for information directed to the carriers would be preempted by federal law. Indeed, the carriers' compliance with such requests by the MPSC would violate federal law and would place the carriers 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 grant the pending motions to dismiss or otherwise close these proceedings 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

Attachments

cc: Mark D. Eyster, Administrative Law Judge
Service List for U-14985

PETER D. KEISLER
Assistant Attorney General, Civil Division
CARL J. NICHOLS
Deputy Assistant Attorney General
DOUGLAS N. LETTER
Terrorism Litigation Counsel
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov
ANDREW H. TANNENBAUM
andrew.tannenbaum@usdoj.gov
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/(202) 514-4263
Fax: (202) 616-8460/(202) 616-8202/(202) 318-2461

Attorneys for Intervenor Defendant United States of America

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, GREGORY HICKS)
CAROLYN JEWEL, and ERIK KNUTZEN)
on Behalf of Themselves and All Others)
Similarly Situated,)

Plaintiffs,)

v.)

AT&T CORP., AT&T INC., and)
DOES 1-20, inclusive,)

Defendants.)

Case No. C 06-0672-VRW

NOTICE OF MOTION AND MOTION TO
DISMISS OR, IN THE ALTERNATIVE,
FOR SUMMARY JUDGMENT
BY THE UNITED STATES OF AMERICA

Judge: The Hon. Vaughn R. Walker
Hearing Date: June 21, 2006
Courtroom: 6, 17th Floor

NOTICE OF MOTION AND MOTION TO DISMISS, OR, IN THE ALTERNATIVE, FOR SUMMARY
JUDGMENT BY THE UNITED STATES OF AMERICA
Case No. C 06-0672-VRW

1 PLEASE TAKE NOTICE that, on June 21, 2006,¹ before the Honorable Vaughn R.
2 Walker, intervenor United States of America will move for an order dismissing this action,
3 pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, or, in the
4 alternative, for summary judgment, pursuant to Rule 56 of the Federal Rules of Civil Procedure.
5 As explained in the United States' unclassified memorandum as well as the memorandum
6 submitted *ex parte* and *in camera*, the United States' invocation of the military and state secrets
7 privilege and of specified statutory privileges requires dismissal of this action, or, in the
8 alternative, summary judgment in favor of the United States.

9 Respectfully submitted,

10 PETER D. KEISLER
11 Assistant Attorney General, Civil Division

12 CARL J. NICHOLS
13 Deputy Assistant Attorney General

14 DOUGLAS N. LETTER
15 Terrorism Litigation Counsel

16 JOSEPH H. HUNT
17 Director, Federal Programs Branch

18 s/Anthony J. Coppolino
19 ANTHONY J. COPPOLINO
20 Special Litigation Counsel
21 tony.coppolino@usdoj.gov

22 s/Andrew H. Tannenbaum
23 ANDREW H. TANNENBAUM
24 Trial Attorney
25 andrew.tannenbaum@usdoj.gov
26 U.S. Department of Justice
27 Civil Division, Federal Programs Branch
28 20 Massachusetts Avenue, NW
Washington, D.C. 20001

24 ¹ The United States has filed an Administrative Motion to Set Hearing Date for the United
25 States' Motions requesting that the Court set the hearing date for this motion and the United
26 States' Motion To Intervene, for June 21, 2006 – the present hearing date for Plaintiffs' Motion
for Preliminary Injunction.

Phone: (202) 514-4782/(202) 514-4263
Fax: (202) 616-8460/(202) 616-8202/(202) 318-2461

Attorneys for Intervenor Defendant United States

DATED: May 12, 2006

NOTICE OF MOTION AND MOTION TO DISMISS, OR, IN THE ALTERNATIVE, FOR SUMMARY
JUDGMENT BY THE UNITED STATES OF AMERICA
Case No. C 06-0672-VRW

1 PETER D. KEISLER
 2 Assistant Attorney General
 3 CARL J. NICHOLS
 4 Deputy Assistant Attorney General
 5 DOUGLAS N. LETTER
 6 Terrorism Litigation Counsel
 7 JOSEPH H. HUNT
 8 Director, Federal Programs Branch
 9 ANTHONY J. COPPOLINO
 10 Special Litigation Counsel
 11 tony.coppolino@usdoj.gov
 12 ANDREW H. TANNENBAUM
 13 andrew.tannenbaum@usdoj.gov
 14 Trial Attorney
 15 U.S. Department of Justice
 16 Civil Division, Federal Programs Branch
 17 20 Massachusetts Avenue, NW
 18 Washington, D.C. 20001
 19 Phone: (202) 514-4782/(202) 514-4263
 20 Fax: (202) 616-8460/(202) 616-8202
 21 *Attorneys for the United States of America*

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

17 TASH HEPTING, GREGORY HICKS,)
 18 CAROLYN JEWEL, and ERIK KNUTZEN,)
 19 On Behalf of Themselves and All Others)
 20 Similarly Situated,)
 21 Plaintiffs,)
 22 v.)
 23 AT&T CORP., AT&T INC., and)
 24 DOES 1-20, inclusive,)
 25 Defendants.)

Case No. C-06-0672-VRW

**MEMORANDUM OF THE
 UNITED STATES IN SUPPORT
 OF THE MILITARY AND
 STATE SECRETS PRIVILEGE
 AND MOTION TO DISMISS OR,
 IN THE ALTERNATIVE, FOR
 SUMMARY JUDGMENT**

Hon. Vaughn R. Walker

26
 27
 28
 MEMORANDUM OF THE UNITED STATES IN SUPPORT
 OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
 OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
 CASE NO. C-06-0672-VRW

(U) INTRODUCTION

(U) The United States of America, through its undersigned counsel, hereby submits this Memorandum of Points and Authorities in support of the assertion of the military and state secrets privilege (commonly known as the “state secrets privilege”)¹ by the Director of National Intelligence (“DNI”), and related statutory privilege assertions by the DNI and the Director of the National Security Agency (“DIRNSA”).² Through these assertions of privilege, the United States seeks to protect certain intelligence activities, information, sources, and methods, implicated by the allegations in this case. The information to be protected is described herein, in a separate memorandum lodged for the Court’s *in camera*, *ex parte* consideration, and in public and classified declarations submitted by the DNI and DIRNSA.³ For the reasons set forth in those submissions, the disclosure of the information to which these privilege assertions apply would cause exceptionally grave harm to the national security of the United States.

(U) In addition, the United States has also moved to intervene in this action, pursuant to Rule 24 of the Federal Rules of Civil Procedure, for the purpose of seeking dismissal of this action or, in the alternative, summary judgment. As set forth below, this case cannot be litigated because adjudication of Plaintiffs’ claims would put at risk the disclosure of privileged national security information.

¹ (U) The phrase “state secrets privilege” is often used in this memorandum to refer collectively to the military and state secrets privilege and the statutory privileges invoked in this case.

² (U) This submission is made pursuant to 28 U.S.C. § 517, as well as pursuant to the Federal Rules of Civil Procedure.

³ (U) The classified declarations of John D. Negroponte, DNI, and Keith B. Alexander, DIRNSA, as well as the separately lodged memorandum for the Court’s *in camera*, *ex parte* consideration, are currently stored in a proper secure location by the Department of Justice and are available for review by the Court upon request.

1 [REDACTED TEXT]

2 (U) The state secrets privilege has long been recognized for protecting information vital
3 to the nation's security or diplomatic relations. See *United States v. Reynolds*, 345 U.S. 1
4 (1953); *Kasza v. Browner*, 133 F.3d 1159 (9th Cir.), cert. denied, 525 U.S. 967 (1998). "Once
5 the privilege is properly invoked and the court is satisfied that there is a reasonable danger that
6 national security would be harmed by the disclosure of state secrets, the privilege is absolute,"
7 and the information at issue must be excluded from disclosure and use in the case. *Kasza*, 133
8 F.3d at 1166. Moreover, if "the 'very subject matter of the action' is a state secret, then the court
9 should dismiss the plaintiff's action based solely on the invocation of the state secrets privilege."
10 *Kasza*, 133 F.3d at 1166. In such cases, "sensitive military secrets will be so central to the
11 subject matter of the litigation that any attempt to proceed will threaten disclosure of the
12 privileged matters." See *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236 (4th Cir. 1985).
13 Dismissal is also necessary when either the plaintiff cannot make out a prima facie case in
14 support of its claims absent the excluded state secrets, or if the privilege deprives the defendant
15 of information that would otherwise provide a valid defense to the claim. *Kasza*, 133 F.3d at
16 1166.
17
18
19

20 [REDACTED TEXT]

21 (U) BACKGROUND

22 A. (U) September 11, 2001

23 (U) On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated
24 attacks along the East Coast of the United States. Four commercial jetliners, each carefully
25 selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda
26 operatives. Those operatives targeted the Nation's financial center in New York with two of the
27
28

1 jetliners, which they deliberately flew into the Twin Towers of the World Trade Center. Al
2 Qaeda targeted the headquarters of the Nation's Armed Forces, the Pentagon, with the third
3 jetliner. Al Qaeda operatives were apparently headed toward Washington, D.C. with the fourth
4 jetliner when passengers struggled with the hijackers and the plane crashed in Shanksville,
5 Pennsylvania. The intended target of this fourth jetliner was most evidently the White House or
6 the Capitol, strongly suggesting that al Qaeda's intended mission was to strike a decapitation
7 blow to the Government of the United States—to kill the President, the Vice President, or
8 Members of Congress. The attacks of September 11 resulted in approximately 3,000 deaths—
9 the highest single-day death toll from hostile foreign attacks in the Nation's history. In addition,
10 these attacks shut down air travel in the United States, disrupted the Nation's financial markets
11 and Government operations, and caused billions of dollars of damage to the economy.
12

13
14 (U) On September 14, 2001, the President declared a national emergency “by reason of
15 the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the
16 continuing and immediate threat of further attacks on the United States.” Proclamation No.
17 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001). The United States also launched a massive military
18 response, both at home and abroad. In the United States, combat air patrols were immediately
19 established over major metropolitan areas and were maintained 24 hours a day until April 2002.
20 The United States also immediately began plans for a military response directed at al Qaeda's
21 training grounds and haven in Afghanistan. On September 14, 2001, both Houses of Congress
22 passed a Joint Resolution authorizing the President “to use all necessary and appropriate force
23 against those nations, organizations, or persons he determines planned, authorized, committed, or
24 aided the terrorist attacks” of September 11. Authorization for Use of Military Force, Pub. L.
25 No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001) (“Cong. Auth.”). Congress also
26
27
28

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRET'S PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 expressly acknowledged that the attacks rendered it “necessary and appropriate” for the United
2 States to exercise its right “to protect United States citizens both at home and abroad,” and
3 acknowledged in particular that the “the President has authority under the Constitution to take
4 action to deter and prevent acts of international terrorism against the United States.” *Id.* pmb1.

5 (U) As the President made clear at the time, the attacks of September 11 “created a state
6 of armed conflict.” Military Order, § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001). Indeed,
7 shortly after the attacks, NATO took the unprecedented step of invoking article 5 of the North
8 Atlantic Treaty, which provides that an “armed attack against one or more of [the parties] shall
9 be considered an attack against them all.” North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat.
10 2241, 2244, 34 U.N.T.S. 243, 246; see also Statement by NATO Secretary General Lord
11 Robertson (Oct. 2, 2001), available at <http://www.nato.int/docu/speech/2001/s011002a.htm> (“[I]t
12 has now been determined that the attack against the United States on 11 September was directed
13 from abroad and shall therefore be regarded as an action covered by Article 5 of the Washington
14 Treaty . . .”). The President also determined that al Qaeda terrorists “possess both the capability
15 and the intention to undertake further terrorist attacks against the United States that, if not
16 detected and prevented, will cause mass deaths, mass injuries, and massive destruction of
17 property, and may place at risk the continuity of the operations of the United States
18 Government,” and he concluded that “an extraordinary emergency exists for national defense
19 purposes.” Military Order, § 1(c), (g), 66 Fed. Reg. at 57833-34.

20
21 **B. (U) The Continuing Terrorist Threat Posed by al Qaeda**

22 (U) With the attacks of September 11, Al Qaeda demonstrated its ability to introduce
23 agents into the United States undetected and to perpetrate devastating attacks. But, as the
24 President has made clear, “[t]he terrorists want to strike America again, and they hope to inflict
25
26
27
28

1 even more damage than they did on September the 11th.” Press Conference of President Bush
2 (Dec. 19, 2005).⁴ For this reason, as the President explained, finding al Qaeda sleeper agents in
3 the United States remains one of the paramount national security concerns to this day. *See id.*

4 (U) Since the September 11 attacks, al Qaeda leaders have repeatedly promised to
5 deliver another, even more devastating attack on America. For example, in October 2002, al
6 Qaeda leader Ayman al-Zawahiri stated in a video addressing the “citizens of the United States”:
7 “I promise you that the Islamic youth are preparing for you what will fill your hearts with
8 horror.” In October 2003, Osama bin Laden stated in a released videotape that “We, God
9 willing, will continue to fight you and will continue martyrdom operations inside and outside the
10 United States” And again in a videotape released on October 24, 2004, bin Laden warned
11 U.S. citizens of further attacks and asserted that “your security is in your own hands.” In recent
12 months, al Qaeda has reiterated its intent to inflict a catastrophic terrorist attack on the United
13 States. On December 7, 2005, al-Zawahiri professed that al Qaeda “is spreading, growing, and
14 becoming stronger,” and that al Qaeda is “waging a great historic battle in Iraq, Afghanistan,
15 Palestine, and even in the Crusaders’ own homes.” Finally, as is well known, since September
16 11, al Qaeda has staged several large-scale attacks around the world, including in Indonesia,
17 Madrid, and London, killing hundreds of innocent people.
18
19
20

21 [REDACTED TEXT]

22 C. (U) Intelligence Challenges After September 11, 2001

23 [REDACTED TEXT]
24
25
26

27 ⁴ (U) Available at [http://www.white-house.gov/news/releases/2005/12/20051219-](http://www.white-house.gov/news/releases/2005/12/20051219-2.html)
28 [2.html](http://www.white-house.gov/news/releases/2005/12/20051219-2.html).

1 D. (U) NSA Activities Critical to Meeting Post-9/11 Intelligence Challenges

2 [REDACTED TEXT]

3 E. (U) Plaintiffs' Claims

4 (U) Against this backdrop, upon the media disclosures in December 2005 of certain post-
5 9/11 intelligence gathering activities, Plaintiffs filed this suit alleging that the Government is
6 conducting a massive surveillance program, vacuuming up and searching the content of
7 communications engaged in by millions of AT&T customers. While clearly putting purported
8 Government activities at issue, *see* Am. Compl. ¶ 3, Plaintiffs filed suit against AT&T, alleging
9 that it illegally provides the NSA with direct access to key facilities and databases and discloses
10 to the Government the content of telephone and electronic communications as well as detailed
11 communications records about millions of customers. *See* Am. Complaint ¶¶ 3-6.

14 (U) Plaintiffs first put at issue NSA's activities in connection with the TSP, which was
15 publicly described by the President in December 2005, alleging that "NSA began a classified
16 surveillance program shortly after September 11, 2001 to intercept the communications within
17 the United States without judicial warrant." *See* Am. Compl. ¶ 32-37. Plaintiffs also allege that
18 as part of this "data mining" program, "the NSA intercepts millions of communications made or
19 received by people inside the United States, and uses powerful computers to scan their contents
20 for particular names, numbers, words, or phrases." *Id.* ¶ 39. Plaintiffs allege in particular that
21 AT&T has assisted the Government in installing "interception devices," "pen registers" and "trap
22 and trace" devices in order to "acquire the content" of communications and receive "dialing,
23 routing, addressing, or signaling information." *Id.* ¶¶ 42-47.

26 (U) Plaintiffs seek declaratory and injunctive relief and damages under various federal
27 and state statutory provisions and the First and Fourth Amendments, Am. Compl. ¶¶ 65-66 &
28

Counts II-VI, and also seek declaratory and injunctive relief under the First and Fourth Amendments on the theory that the Government has instigated, directed, or tacitly approved the alleged actions by AT&T, and that AT&T acts as an instrument or agent of the Government. *Id.* ¶¶ 66, 82, 85 & Count I. Finally, Plaintiffs have also moved for a preliminary injunction that would, *inter alia*, enjoin AT&T “from facilitating the interception, use, or disclosure of its customers’ communications by or to the United States Government,” except pursuant to a court order or an emergency authorization of the Attorney General. *See* [Proposed] Order Granting Preliminary Injunction (Docket No. 17) ¶ 3.

(U) ARGUMENT

[REDACTED TEXT]

I. (U) THE STATE SECRETS PRIVILEGE BARS USE OF PRIVILEGED INFORMATION REGARDLESS OF A LITIGANT’S NEED.

(U) The ability of the executive to protect military or state secrets from disclosure has been recognized from the earliest days of the Republic. *See Totten v. United States*, 92 U.S. 105 (1875); *United States v. Burr*, 25 F. Cas. 30 (C.C.D. Va. 1807); *Reynolds*, 345 U.S. at 6-7. The privilege derives from the President’s Article II powers to conduct foreign affairs and provide for the national defense. *United States v. Nixon*, 418 U.S. 683, 710 (1974). Accordingly, it “must head the list” of evidentiary privileges. *Halkin I*, 598 F.2d at 7.

A. (U) Procedural Requirements

(U) As a procedural matter, “[t]he privilege belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party.” *Reynolds*, 345 U.S. at 7; *see also Kasza*, 133 F.3d at 1165. “There must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by the officer.” *Reynolds*, 345 U.S. at 7-8 (footnotes omitted). Thus, the responsible agency head

1 must personally consider the matter and formally assert the claim of privilege.

2 **B. (U) Information Covered**

3 (U) The privilege protects a broad range of state secrets, including information that would
4 result in "impairment of the nation's defense capabilities, disclosure of intelligence-gathering
5 methods or capabilities, and disruption of diplomatic relations with foreign Governments."
6 *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983), *cert. denied sub nom. Russo v. Mitchell*,
7 465 U.S. 1038 (1984) (footnotes omitted); *accord Kasza*, 133 F.3d at 1166 ("[T]he Government
8 may use the state secrets privilege to withhold a broad range of information;"); *see also Halkin v.*
9 *Helms (Halkin II)*, 690 F.2d 977, 990 (D.C. Cir. 1982) (state secrets privilege protects
10 intelligence sources and methods involved in NSA surveillance). In addition, the privilege
11 extends to protect information that, on its face, may appear innocuous but which in a larger
12 context could reveal sensitive classified information. *Kasza*, 133 F.3d at 1166.

15 It requires little reflection to understand that the business of foreign intelligence
16 gathering in this age of computer technology is more akin to the construction of a
17 mosaic than it is to the management of a cloak and dagger affair. Thousands of
18 bits and pieces of seemingly innocuous information can be analyzed and fitted
19 into place to reveal with startling clarity how the unseen whole must operate.

20 *Halkin I*, 598 F.2d at 8. "Accordingly, if seemingly innocuous information is part of a classified
21 mosaic, the state secrets privilege may be invoked to bar its disclosure and the court cannot order
22 the Government to disentangle this information from other classified information." *Kasza*, 133
23 F.3d at 1166.

24 **C. (U) Standard of Review**

25 (U) An assertion of the state secrets privilege "must be accorded the 'utmost deference'
26 and the court's review of the claim of privilege is narrow." *Kasza*, 133 F.3d at 1166. Aside
27 from ensuring that the privilege has been properly invoked as a procedural matter, the sole
28

1 determination for the court is whether, “under the particular circumstances of the case, ‘there is a
2 reasonable danger that compulsion of the evidence will expose military matters which, in the
3 interest of national security, should not be divulged.’” *Kasza*, 133 F.3d at 1166 (quoting
4 *Reynolds*, 345 U.S. at 10); *see also In re United States*, 872 F.2d 472, 475-76 (D.C. Cir. 1989);
5 *Tilden v. Tenet*, 140 F. Supp. 2d 623, 626 (E.D. Va. 2000).

6
7 (U) Thus, in assessing whether to uphold a claim of privilege, the court does not balance
8 the respective needs of the parties for the information. Rather, “[o]nce the privilege is properly
9 invoked and the court is satisfied that there is a reasonable danger that national security would be
10 harmed by the disclosure of state secrets, the privilege is absolute[.]” *Kasza*, 133 F.3d at 1166;
11 *see also In re Under Seal*, 945 F.2d at 1287 n.2 (state secrets privilege “renders the information
12 unavailable regardless of the other party’s need in furtherance of the action”); *Northrop Corp. v.*
13 *McDonnell Douglas Corp.*, 751 F.2d 395, 399 (D.C. Cir. 1984) (state secrets privilege “cannot
14 be compromised by any showing of need on the part of the party seeking the information”);
15 *Ellsberg*, 709 F.2d at 57 (“When properly invoked, the state secrets privilege is absolute. No
16 competing public or private interest can be advanced to compel disclosure of information found
17 to be protected by a claim of privilege.”). The court may consider the necessity of the
18 information to the case only in connection with assessing the sufficiency of the Government’s
19 showing that there is a reasonable danger that disclosure of the information at issue would harm
20 national security. “[T]he more plausible and substantial the Government’s allegations of danger
21 to national security, in the context of all the circumstances surrounding the case, the more
22 deferential should be the judge’s inquiry into the foundations and scope of the claim.” *Id.* at 59.

23
24
25
26 Where there is a strong showing of necessity, the claim of privilege should not be
27 lightly accepted, but even the most compelling necessity cannot overcome the
28 claim of privilege if the court is ultimately satisfied that military secrets are at
stake.

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 *Reynolds*, 345 U.S. at 11; *Kasza*, 133 F.3d at 1166.

2 (U) Judicial review of whether the claim of privilege has been properly asserted and
3 supported does not require the submission of classified information to the court for *in camera*, *ex*
4 *parte* review. In particular, where it is possible to satisfy the court, from all the circumstances of
5 the case, that there is a reasonable danger that compulsion of the evidence will expose state
6 secrets which, in the interest of national security, should not be divulged, "the occasion for the
7 privilege is appropriate, and the court should not jeopardize the security which the privilege is
8 meant to protect by insisting upon an examination of the evidence, even by the judge alone, in
9 chambers." *Reynolds*, 345 U.S. at 8. Indeed, one court has observed that *in camera*, *ex parte*
10 review itself may not be "entirely safe."

13 It is not to slight judges, lawyers or anyone else to suggest that any such
14 disclosure carries with it serious risk that highly sensitive information may be
15 compromised. In our own chambers, we are ill equipped to provide the kind of
security highly sensitive information should have.

16 *Clift v. United States*, 597 F.2d 826, 829 (2d Cir. 1979) (quoting *Alfred A. Knopf, Inc. v. Colby*,
17 509 F.2d 1362, 1369 (4th Cir.), *cert. denied*, 421 U.S. 992 (1975)).

19 (U) Nonetheless, the submission of classified declarations for *in camera*, *ex parte* review
20 is "unexceptional" in cases where the state secrets privilege is invoked. *Kasza*, 133 F.3d at 1169
21 (citing *Black v. United States*, 62 F.3d 1115 (8th Cir. 1995), *cert. denied*, 517 U.S. 1154 (1996));
22 see *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544 (2d Cir. 1991); *Fitzgerald v.*
23 *Penthouse Int'l, Ltd.*, 776 F.2d 1236 (4th Cir. 1985); *Molerio v. FBI*, 749 F.2d 815, 819, 822
24 (D.C. Cir. 1984); *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 281 (4th Cir. 1980) (en
25 banc); see also, e.g., *In re United States*, 872 F.2d at 474 (classified declaration of assistant
26 director of the FBI's Intelligence Division submitted for *in camera* review in support of Attorney
27

28
MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

General's formal invocation of state secrets privilege).

II. (U) THE UNITED STATES PROPERLY HAS ASSERTED THE STATE SECRETS PRIVILEGE AND ITS CLAIM OF PRIVILEGE SHOULD BE UPHOLD.

A. (U) The United States Properly Has Asserted the State Secrets Privilege.

(U) It cannot be disputed that the United States properly has asserted the state secrets privilege in this case. The Director of National Intelligence, who bears statutory authority as head of the United States Intelligence Community to protect intelligence sources and methods, *see* 50 U.S.C. § 403-1(i)(1), has formally asserted the state secrets privilege after personal consideration of the matter. *See Reynolds*, 345 U.S. at 7-8.⁵ DNI Negroponte has submitted an unclassified declaration and an *in camera*, *ex parte* classified declaration, both of which state that the disclosure of the intelligence information, sources, and methods described herein would cause exceptionally grave harm to the national security of the United States. *See Public and In Camera, Ex Parte* Declarations of John D. Negroponte, Director of National Intelligence. Based on this assertion of privilege by the head of the United States intelligence community, the Government's claim of privilege has been properly lodged.

B. (U) The United States Has Demonstrated that There is a Reasonable Danger that Disclosure of the Intelligence Information, Sources, and Methods Implicated by Plaintiffs' Claims Would Harm the National Security of the United States.

(U) The United States also has demonstrated that there is a reasonable danger that disclosure of the information subject to the state secrets privilege would harm U.S. national security. *Kasza*, 133 F.3d at 1170. While "the Government need not demonstrate that injury to

⁵ (U) *See* 50 U.S.C. § 401a(4) (including the National Security Agency is included in the United States "Intelligence Community").

1 the national interest will inevitably result from disclosure," *Ellsberg, supra*, 709 F.2d at 58, the
2 showing made here is more than reasonable, and highly compelling.

3 (U) DNI Negroponte, supported by the *Ex Parte, In Camera* Declaration of General
4 Alexander, has asserted the state secrets privilege and demonstrated the exceptional harm that
5 would be caused to U.S. national security interests by disclosure of each of the following the
6 categories of privileged information at issue in this case.

7 [REDACTED TEXT]

8
9 (U) Each of the foregoing categories of information is subject to DNI Negroponte's state
10 secrets privilege claim, and he and General Alexander have amply demonstrated a reasoned basis
11 that disclosure of this information would cause exceptionally grave damage to the national
12 security and, therefore, that this information should be excluded from this case.

13
14 **C. (U) Statutory Privilege Claims Have Also Been Properly Raised in This Case.**

15 (U) Two statutory protections also apply to the intelligence-related information, sources
16 and methods described herein, and both have been properly invoked here as well. First, Section
17 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified
18 at 50 U.S.C. § 402 note, provides:

19
20 [N]othing in this Act or any other law . . . shall be construed to require the
21 disclosure of the organization or any function of the National Security Agency,
22 of any information with respect to the activities thereof, or of the names, titles,
salaries, or number of persons employed by such agency.

23 *Id.* Section 6 reflects a "congressional judgment that in order to preserve national security,
24 information elucidating the subjects specified ought to be safe from forced exposure." *The*
25 *Founding Church of Scientology of Washington, D.C., Inc. v. Nat'l Security Agency*, 610 F.2d
26 824, 828 (D.C. Cir. 1979); *accord Hayden v. Nat'l Security Agency*, 608 F.2d 1381, 1389 (D.C.
27 Cir. 1979). In enacting Section 6, Congress was "fully aware of the 'unique and sensitive'
28

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 activities of the [NSA] which require 'extreme security measures.'" *Hayden*, 608 F.2d at 1390
2 (citing legislative history). Thus, "[t]he protection afforded by section 6 is, by its very terms,
3 absolute. If a document is covered by section 6, NSA is entitled to withhold it. . . ." *Linder v.*
4 *Nat'l Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996).

5 (U) The second applicable statute is Section 102A(i)(1) of the Intelligence Reform and
6 Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified
7 at 50 U.S.C. § 403-1(i)(1). This statute requires the Director of National Intelligence to "protect
8 intelligence sources and methods from unauthorized disclosure. The authority to protect
9 intelligence sources and methods from disclosure is rooted in the "practical necessities of
10 modern intelligence gathering," *Fitzgibbon v. CIA*, 911 F.2d 755, 761 (D.C. Cir. 1990), and has
11 been described by the Supreme Court as both "sweeping," *CIA v. Sims*, 471 U.S. 159, 169
12 (1985), and "wideranging," *Snepp v. United States*, 444 U.S. 507, 509 (1980). Sources and
13 methods constitute "the heart of all intelligence operations," *Sims*, 471 U.S. at 167, and "[i]t is
14 the responsibility of the [intelligence community], not that of the judiciary to weigh the variety
15 of complex and subtle factors in determining whether disclosure of information may lead to an
16 unacceptable risk of compromising the . . . intelligence-gathering process." *Id.* at 180.

17 (U) These statutory privileges have been properly asserted as to any intelligence-related
18 information, sources and methods implicated by Plaintiffs' claims and the information covered
19 by these privilege claims are at least co-extensive with the assertion of the state secrets privilege
20 by the DNI. See Public Declaration of John D. Negroponte, Director of National Intelligence,
21 and Public Declaration of Keith T. Alexander, Director of the National Security Agency.

22 **III. (U) THE STATE SECRETS PRIVILEGE REQUIRES DISMISSAL OF THIS**
23 **ACTION.**

24 (U) Once the court has upheld a claim of the state secrets privilege, the evidence and
25

1 information identified in the privilege assertion is removed from the case, and the Court must
2 undertake a separate inquiry to determine the consequences of this exclusion on further
3 proceedings.

4 (U) If “the ‘very subject matter of the action’ is a state secret, then the court should
5 dismiss the plaintiff’s action based solely on the invocation of the state secrets privilege.” *Kasza*,
6 133 F.3d at 1166 (citing *Reynolds*, 345 U.S. at 11 n. 26); *see also Totten v. United States*, 92 U.S.
7 (2 Otto) 105, 107, 23 L.Ed. 605 (1875) (“[P]ublic policy forbids the maintenance of any suit in a
8 court of justice, the trial of which would inevitably lead to the disclosure of matters which the
9 law itself regards as confidential, and respecting which it will not allow the confidence to be
10 violated.”); *Weston v. Lockheed Missiles & Space Co.*, 881 F.2d 814, 816 (9th Cir. 1989)
11 (recognizing that state secrets privilege alone can be the basis of dismissal of a suit). In such
12 cases, “sensitive military secrets will be so central to the subject matter of the litigation that any
13 attempt to proceed will threaten disclosure of the privileged matters.” *Fitzgerald*, 776 F.2d at
14 1241-42. *See also Maxwell v. First National Bank of Maryland*, 143 F.R.D. 590, 598-99 (D. Md.
15 1992); *Edmonds v. U.S. Department of Justice*, 323 F. Supp. 2d 65, 77-82 (D.D.C. 2004), *aff’d*,
16 161 Fed. Appx. 6, 045286 (D.C. Cir. May 6, 2005) (*per curiam* judgment), *cert. denied*, 126 S.
17 Ct. 734 (2005); *Tilden*, 140 F. Supp. 2d at 626.

21 (U) Even if the very subject matter of an action is not a state secret, if the plaintiff cannot
22 make out a prima facie case in support of its claims absent the excluded state secrets, the case
23 must be dismissed. *See Kasza*, 133 F.3d at 1166; *Halkin II*, 690 F.2d at 998-99; *Fitzgerald*, 776
24 F.2d at 1240-41. And if the privilege “deprives the *defendant* of information that would
25 otherwise give the defendant a valid defense to the claim, then the court may grant summary
26 judgment to the defendant.” *Kasza*, 133 F.3d at 1166 (quoting *Bareford v. General Dynamics*
27
28

1 *Corp.*, 973 F.2d 1138, 1141 (5th Cir. 1992)); *see also Molerio v. FBI*, 749 F.2d 815, 825 (D.C.
2 Cir. 1984) (granting summary judgment where state secrets privilege precluded the Government
3 from using a valid defense).

4 [REDACTED TEXT]

5 A. (U) Further Litigation Would Inevitably Risk the Disclosure of State Secrets.

6 [REDACTED TEXT]

7
8 B. (U) Information Subject to the State Secrets Privilege is
9 Necessary to Adjudicate Plaintiffs' Claims.

10 (U) Beyond the foregoing concerns, it should also be apparent that any attempt to litigate
11 the merits of the Plaintiffs' claims will require the disclosure of information covered by the state
12 secrets assertion. Adjudicating each claim in the Amended Complaint would require
13 confirmation or denial of the existence, scope, and potential targets of alleged intelligence
14 activities, as well as AT&T's alleged involvement in such activities. Because such information
15 cannot be confirmed or denied without causing exceptionally grave damage to the national
16 security, every step in this case—either for Plaintiffs to prove their claims, for Defendants to
17 defend them, or for the United States to represent its interests—runs into privileged information.
18
19

20 1. (U) Plaintiffs Cannot Establish Standing

21 (U) As a result of the Government's state secrets assertion, Plaintiffs will not be able to
22 prove that they have standing to litigate their claims. Plaintiffs, of course, bear the burden of
23 establishing standing and must, at an "irreducible constitutional minimum," demonstrate (1) an
24 injury-in-fact, (2) a causal connection between the injury and the conduct complained of, and (3)
25 a likelihood that the injury will be redressed by a favorable decision. *Lujan v. Defenders of*
26 *Wildlife*, 504 U.S. 555, 560-61 (1992). In meeting that burden, the named Plaintiffs must
27
28

1 demonstrate an actual or imminent—not speculative or hypothetical—injury that is particularized
2 as to them; they cannot rely on alleged injuries to unnamed members of a purported class.⁶
3 Moreover, to obtain prospective relief, Plaintiffs must show that they are “immediately in danger
4 of sustaining some direct injury” as the result of the challenged conduct. *City of Los Angeles v.*
5 *Lyons*, 461 U.S. 95, 102 (1983); *O’Shea v. Littleton*, 414 U.S. 488, 495-96 (1974).⁷ In addition
6 to the constitutional requirements of Article III, Plaintiffs must also satisfy prudential standing
7 requirements, including that they “assert [their] own legal interests rather than those of third
8 parties,” *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 804 (1985), and that their claim not be a
9 “generalized grievance” shared in substantially equal measure by all or a large class of citizens.
10 *Warth v. Seldin*, 422 U.S. 499 (1975).
11

12
13 (U) Plaintiffs cannot prove these elements without information covered by the state
14 secrets assertion.⁸ The Government’s privilege assertion covers any information tending to
15

16 ⁶ (U) *See, e.g., Warth v. Seldin*, 422 U.S. 490, 502 (1975) (the named plaintiffs in an
17 action “must allege and show that they personally have been injured, not that injury has been
18 suffered by other, unidentified members of the class to which they belong and which they
19 purport to represent”).

20 ⁷ (U) Standing requirements demand the “strictest adherence” when, like here,
21 constitutional questions are presented and “matters of great national significance are at stake.”
22 *Elk Grove Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 11 (2004); *see also Raines v. Byrd*, 521
23 U.S. 811, 819-20 (1997) (“[O]ur standing inquiry has been especially rigorous when reaching the
24 merits of the dispute would force us to decide whether an action taken by one of the other two
25 branches of the Federal Government was unconstitutional.”); *Schlesinger v. Reservists Comm. to*
26 *Stop the War*, 418 U.S. 208, 221 (1974) (“[W]hen a court is asked to undertake constitutional
27 adjudication, the most important and delicate of its responsibilities, the requirement of concrete
28 injury further serves the function of insuring that such adjudication does not take place
unnecessarily.”).

29 ⁸ (U) The focus herein is on Plaintiffs’ inability to prove standing because it is their
30 burden to demonstrate jurisdiction. *See Lujan*, 504 U.S. at 561. Dismissal of this action,
31 however, is also required for the equally important reason that AT&T and the Government
32 would not be able to present any evidence disproving standing on any claim without revealing
33 information covered by the state secrets privilege assertion (e.g., whether or not a particular
34 person’s communications were intercepted). *See Halkin I*, 598 F.2d at 11 (rejecting plaintiffs’

1 confirm or deny (a) the alleged intelligence activities, (b) whether AT&T was involved with any
2 such activity, and (c) whether a particular individual's communications were intercepted as a
3 result of any such activity. *See* Public Declaration of John D. Negroponte. Without these
4 facts—which should be removed from the case as a result of the state secrets assertion—
5 Plaintiffs cannot establish any alleged injury that is fairly traceable to AT&T. Thus, regardless
6 of whether they adequately allege such facts, Plaintiffs ultimately will not be able to prove
7 injury-in-fact or causation.⁹

9 (U) In such circumstances, courts have held that the assertion of the state secrets privilege
10 requires dismissal of the case. In *Halkin I*, for example, a number of individuals and
11 organizations claimed that they were subject to unlawful surveillance by the NSA and CIA
12 (among other agencies) due to their opposition to the Vietnam War. *See* 598 F.2d at 3. The D.C.

14
15 argument that the acquisition of a plaintiff's communications may be presumed from the
16 existence of a name on a watchlist, because "such a presumption would be unfair to the
individual defendants who would have no way to rebut it").

17 ⁹ (U) To the extent Plaintiffs challenge the TSP, *see, e.g.*, Am. Compl. 32-37, their
18 allegations are insufficient on their face to establish standing even apart from the state secrets
19 issue because Plaintiffs fail to demonstrate that they fall anywhere near the scope of that
20 program. Plaintiffs do not claim to be, or to communicate with, members or affiliates of al
21 Qaeda—indeed, Plaintiffs expressly *exclude* from their purported class any foreign powers or
22 agents of foreign powers, "including without limitation anyone who knowingly engages in
23 sabotage or international terrorism, or activities that are in preparation therefore." Am. Compl.
24 ¶ 70. The named Plaintiffs thus are in no different position from any other citizen or AT&T
25 subscriber who falls *outside* the narrow scope of the TSP but nonetheless disagrees with the
26 program. Such a generalized grievance is clearly insufficient to support either constitutional or
27 prudential standing to challenge the TSP. *See Halkin II*, 690 F.2d at 1001-03 (holding that
28 individuals and organizations opposed to the Vietnam War lacked standing to challenge
intelligence activities because they did not adequately allege that they were (or immediately
would be) subject to such activities; thus, their claims were "nothing more than a generalized
grievance against the intelligence-gathering methods sanctioned by the President") (internal
quotation marks and citation omitted); *United Presbyterian Church v. Reagan*, 738 F.2d 1375,
1380 (D.C. Cir. 1984) (rejecting generalized challenge to alleged unlawful surveillance). To the
extent Plaintiffs allege classified intelligence activities beyond the TSP, Plaintiffs could not
prove such allegations in light of the state secrets assertion.

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 Circuit upheld an assertion of the state secrets privilege regarding the identities of individuals
2 subject to NSA surveillance, rejecting the plaintiffs' argument that the privilege could not extend
3 to the "mere fact of interception," *id.* at 8, and despite significant public disclosures about the
4 surveillance activities at issue, *id.* at 10.¹⁰ A similar state secrets assertion with respect to the
5 identities of individuals subject to CIA surveillance was upheld in *Halkin II*. See 690 F.2d at
6 991. As a result of these privilege assertions in both *Halkin I* and *Halkin II*, the D.C. Circuit held
7 that the plaintiffs were incapable of demonstrating that they had standing to challenge the alleged
8 surveillance. See *id.* at 997.¹¹ Significantly, the court held that the fact of such surveillance
9 could not be proven even if the CIA had actually requested NSA to intercept the plaintiffs'
10 communications by including their names on a "watchlist" sent to NSA—a fact which was not
11 covered by the state secrets assertion in that case. See *id.* at 999-1000 ("[T]he absence of proof
12 of actual acquisition of appellants' communications is fatal to their watchlisting claims."). The
13 court thus found dismissal warranted, even though the complaint alleged actual interception of
14
15
16

17 ¹⁰ (U) As the court of appeals recognized, the "identification of the individuals or
18 organizations whose communications have or have not been acquired presents a reasonable
19 danger that state secrets would be revealed . . . [and] can be useful information to a sophisticated
intelligence analyst." *Halkin I*, 598 F.2d at 9.

20 ¹¹ (U) See *Halkin II*, 690 F.2d at 998 ("We hold that appellants' inability to adduce proof
21 of actual acquisition of their communications now prevents them from stating a cognizable claim
22 in the federal courts. In particular, we find appellants incapable of making the showing
23 necessary to establish their standing to seek relief."); *id.* at 997 (quoting district court's ruling
24 that "plaintiffs cannot show any injury from having their names submitted to NSA because NSA
25 is prohibited from disclosing whether it acquired any of plaintiffs' communications"); *id.* at 990
26 ("Without access to the facts about the identities of particular plaintiffs who were subjected to
27 CIA surveillance (or to NSA interception at the instance of the CIA), direct injury in fact to any
28 of the plaintiffs would not have been susceptible of proof."); *id.* at 987 ("Without access to
documents identifying either the subjects of . . . surveillance or the types of surveillance used
against particular plaintiffs, the likelihood of establishing injury in fact, causation by the
defendants, violations of substantive constitutional provisions, or the quantum of damages was
clearly minimal."); *Halkin I*, 598 F.2d at 7 ("[T]he acquisition of the plaintiffs' communication is
a fact vital to their claim," and "[n]o amount of ingenuity of counsel . . . can outflank the
Government's objection that disclosure of this fact is protected by privilege.").

1 plaintiffs' communications, because the plaintiffs' alleged injuries could be no more than
2 speculative in the absence of their ability to prove that such interception occurred. *Id.* at 999,
3 1001.¹²

4 (U) Similarly, in *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983), a group of
5 individuals filed suit after learning during the course of the "Pentagon Papers" criminal
6 proceedings that one or more of them had been subject to warrantless electronic surveillance.
7 Although two such wiretaps were admitted, the Attorney General asserted the state secrets
8 privilege, refusing to disclose to the plaintiffs whether any other such surveillance occurred. *See*
9 *id.* at 53-54. As a result of the privilege assertion, the court upheld the district court's dismissal
10 of the claims brought by the plaintiffs the Government had not admitted overhearing, because
11 those plaintiffs could not prove actual injury. *See id.* at 65.

14 (U) The same result is required here. In light of the state secrets assertion, Plaintiffs
15 cannot prove that their communications were intercepted or disclosed by AT&T, and thus they
16 cannot meet their burden to establish standing. Accordingly, like other similar cases before it,
17 this action must be dismissed.¹³

20 ¹² (U) Because the CIA conceded that nine plaintiffs were subjected to certain types of
21 non-NSA surveillance, the D.C. Circuit held that those plaintiffs had demonstrated an injury-in-
22 fact. *See Halkin II*, 690 F.2d at 1003. Nonetheless, the nine plaintiffs were precluded from
23 seeking injunctive and declaratory relief because they could not demonstrate the likelihood of
future injury or a live controversy in light of the fact that the CIA had terminated the specific
intelligence methods at issue. *See id.* at 1005-09.

24 ¹³ (U) Plaintiffs cannot overcome this fundamental standing bar simply by alleging that
25 their speech has been chilled as the result of their own subjective fear of Government
26 surveillance. *See* Plaintiffs' Memorandum of Points and Authorities in Support of Motion for
27 Preliminary Injunction at 25. Specifics about this alleged chilling effect are provided with
28 respect to only one plaintiff, Carolyn Jewel, who claims that she has refrained from responding
openly about Islam or U.S. foreign policy in e-mails to a Muslim individual in Indonesia, and
that she has decided against using the Internet to conduct certain research for her action and
futuristic romance novels. *See id.* at 26. Plaintiffs offer no explanation as to how this admitted
MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 [REDACTED TEXT]

2 2. (U) Plaintiffs' Statutory Claims Cannot Be
3 Proven or Defended Without State Secrets.

4 [REDACTED TEXT]

5 (U) To prove their FISA claim (as alleged in Count I), Plaintiffs would have to show that
6 AT&T intentionally acquired, under color of law and by means of a surveillance device within
7 the United States, the contents of one or more wire communications to or from Plaintiffs. *See*
8 Am Compl. ¶¶ 93–94; 50 U.S.C. §§ 1801(f), 1809, 1810. Likewise, to prove their claim under
9 18 U.S.C. § 2511 (as alleged in Count III), Plaintiffs would have to demonstrate that AT&T
10 intentionally intercepted, disclosed, used, and/or divulged the contents of Plaintiffs' wire or
11 electronic communications. *See* Am. Compl. ¶¶ 102–07. Plaintiffs' claims under 47 U.S.C.
12 § 605, 18 U.S.C. § 2702, and Cal. Bus. & Prof. Code §§ 17200, *et seq*, all require similar proof:
13 the acquisition and/or disclosure of Plaintiffs' communications and related information. Any
14 information tending to confirm or deny the alleged activities, or any alleged AT&T involvement,
15 is subject to the state secrets privilege.
16

17
18 (U) In addition to proving actual interception or disclosure to the NSA of their
19 communications, Plaintiffs must also prove, for each of their statutory claims, that any alleged
20 interception or disclosure was not authorized by the Government. In particular, 18 U.S.C.
21 § 2511(2)(a)(ii) provides:
22

23
24 “self-censorship” makes any sense in light of the acknowledged limitation of the TSP to
25 international communications actually conducted by al Qaeda-affiliated individuals, as opposed
26 to a mass targeting of particular *topics* of conversation or research. *Id.* In any event, Plaintiffs'
27 claim of a chilling effect is foreclosed by *Laird v. Tatum*, 408 U.S. 1 (1972), which squarely
28 rejected the assertion of a subjective chill caused by the mere existence of an intelligence
program as a basis to challenge that program. *See* 408 U.S. at 13-14 (“Allegations of a
subjective chill are not an adequate substitute for a claim of specific present objective harm or a
threat of specific future harm.”) (internal quotation marks omitted).

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

- (A) a court order directing such assistance signed by the authorizing judge, or
- (B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.

(U) If a court order or Government certification is provided, the telecommunications provider is absolutely immune from liability in any case:

No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter.

18 U.S.C. § 2511(2)(a)(ii).¹⁴

(U) As AT&T has correctly explained, the absence of a court order or Government certification under section 2511(2)(a)(ii) is an element of Plaintiffs' claims. *See* AT&T's Motion to Dismiss Amended Complaint at 7-8. Thus, Plaintiffs bear the burden of alleging and proving the lack of such authorization. *See* Senate Report No. 99-541, reprinted in 1986 U.S.C.C.A.N. 3555, 3580 (1986) (stating that a plaintiff "must allege" the absence of a court order or certification; otherwise "the defendant can move to dismiss the complaint for failure to state a claim upon which relief can be granted"). Notably, Plaintiffs fail to meet that burden on the face of their pleadings; they do not specifically allege that AT&T, if it assisted with any alleged

¹⁴ (U) *See also*, e.g., 18 U.S.C. § 2703(e) (same); 50 U.S.C. § 1809 (prohibiting electronic surveillance under color of law "except as authorized by statute"); 18 U.S.C. § 2511 (prohibiting intercepts "[e]xcept as otherwise specifically provided in this chapter").

1 activity, acted without Government authorization. This action may be dismissed on that basis
2 alone. *See* AT&T's Motion to Dismiss Amended Complaint at 7-8. But even if Plaintiffs
3 speculated and alleged the absence of section 2511(2)(a)(ii) authorization, they could not meet
4 their burden of proof on the issue because information confirming or denying AT&T's
5 involvement in alleged intelligence activities is covered by the state secrets assertion.

6 [REDACTED TEXT]
7

8 **3. (U) Plaintiffs' Fourth Amendment Claim Cannot Be Adjudicated**
9 **Without State Secrets**

10 (U) Plaintiffs' Fourth Amendment claim also cannot be proven or defended without
11 information covered by the state secrets assertion. Specifically, Plaintiffs allege that they have a
12 reasonable expectation of privacy in the contents of, and records pertaining to, their
13 communications, and that their rights were violated when AT&T allegedly intercepted or
14 disclosed such communications and records at the instigation of the Government and without
15 lawful authorization. *See* Am. Compl. ¶¶ 78-89.

17 (U) In their preliminary injunction motion, which is focused on Internet communications,
18 Plaintiffs further claim that, "[a]s an agent of the Government," AT&T is engaged in "wholesale
19 copying of vast amounts of communications carried by its WorldNet Internet service." *Pls.*
20 *Prelim. Inj. Mem.* at 25. Plaintiffs assert that the alleged surveillance violates the Fourth
21 Amendment because it involves "an automated 'rummaging' through the millions of private
22 communications passing over AT&T's fiber optic network at the discretion of NSA staff." *See*
23 *id.* at 27. Plaintiffs simply assume that a warrant is required for any and all of the surveillance
24 activities alleged in their Complaint. *See id.*

25 [REDACTED TEXT]
26

27 (U) The requirement of a warrant supported by probable cause is not universal but turns
28

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 on the particular circumstances at issue. The Supreme Court has made clear that, while a search
2 must be supported, as a general matter, by a warrant issued upon probable cause, it has
3 repeatedly “reaffirm[ed] a longstanding principle that neither a warrant nor probable cause, nor,
4 indeed, any measure of individualized suspicion, is an indispensable component of
5 reasonableness in every circumstance.” *National Treasury Employees Union v. Von Raab*, 489
6 U.S. 656, 665 (1989).

8 (U) For example, both before and after the enactment of the Foreign Intelligence
9 Surveillance Act, every federal appellate court to consider the issue has concluded that, even in
10 peacetime, the President has inherent constitutional authority, consistent with the Fourth
11 Amendment, to conduct searches for foreign intelligence purposes without securing a judicial
12 warrant. *See In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) (“[A]ll
13 the other courts to have decided the issue [have] held that the President did have inherent
14 authority to conduct warrantless searches to obtain foreign intelligence information *We take*
15 *for granted that the President does have that authority and, assuming that is so, FISA could not*
16 *encroach on the President’s constitutional power.*”) (emphasis added); *accord, e.g., United*
17 *States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d
18 593 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973). *But cf.*
19 *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc) (dictum in plurality opinion
20 suggesting that a warrant would be required even in a foreign intelligence investigation).

23 (U) In *United States v. United States District Court*, 407 U.S. 297 (1972) (“*Keith*”), the
24 Supreme Court concluded that the Fourth Amendment’s warrant requirement applies to
25 investigations of wholly *domestic* threats to security—such as domestic political violence and
26 other crimes. But the Court made clear that it was not addressing the President’s authority to
27
28

1 conduct *foreign* intelligence surveillance (even within the United States) without a warrant and
2 that it was expressly reserving that question: “[T]he instant case requires no judgment on the
3 scope of the President’s surveillance power with respect to the activities of foreign powers,
4 within or without this country.” *Id.* at 308; *see also id.* at 321-22 & n.20 (“We have not
5 addressed, and express no opinion as to, the issues which may be involved with respect to
6 activities of foreign powers or their agents.”).¹⁵ That *Keith* does not apply in the context of
7 protecting against a foreign attack has been confirmed by the lower courts. After *Keith*, each of
8 the three courts of appeals that have squarely considered the question has concluded—expressly
9 taking the Supreme Court’s decision into account—that the President has inherent authority to
10 conduct warrantless surveillance in the foreign intelligence context. *See, e.g., Truong Dinh*
11 *Hung*, 629 F.2d at 913-14; *Butenko*, 494 F.2d at 603; *Brown*, 484 F.2d 425-26. As one court put
12 it:
13
14

15 [F]oreign intelligence gathering is a clandestine and highly unstructured activity,
16 and the need for electronic surveillance often cannot be anticipated in advance.
17 Certainly occasions arise when officers, acting under the President’s authority, are
18 seeking foreign intelligence information, where exigent circumstances would
19 excuse a warrant. To demand that such officers be so sensitive to the nuances of
20 complex situations that they must interrupt their activities and rush to the nearest
21 available magistrate to seek a warrant would seriously fetter the Executive in the
22 performance of his foreign affairs duties.

21 ¹⁵ (U) *Keith* made clear that one of the significant concerns driving the Court’s
22 conclusion in the domestic security context was the inevitable connection between perceived
23 threats to domestic security and political dissent. As the Court explained: “Fourth Amendment
24 protections become the more necessary when the targets of official surveillance may be those
25 suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where
26 the Government attempts to act under so vague a concept as the power to protect ‘domestic
27 security.’” *Keith*, 407 U.S. at 314; *see also id.* at 320 (“Security surveillances are especially
28 sensitive because of the inherent vagueness of the domestic security concept, the necessarily
broad and continuing nature of intelligence gathering, and the temptation to utilize such
surveillances to oversee political dissent.”). Surveillance of domestic groups raises a First
Amendment concern that generally is not present when the subjects of the surveillance are
foreign powers or their agents.

1 *Butenko*, 494 F.2d 605.

2
3 (U) Beyond this, the Supreme Court has held that the warrant requirement is inapplicable
4 in situations involving “special needs” that go beyond a routine interest in law enforcement.
5 *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995) (there are circumstances ““when special
6 needs, beyond the normal need for law enforcement, make the warrant and probable-cause
7 requirement impracticable”) (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)); *Illinois v.*
8 *McArthur*, 531 U.S. 326, 330 (2001) (“When faced with special law enforcement needs,
9 diminished expectations of privacy, minimal intrusions, or the like, the Court has found that
10 certain general, or individual, circumstances may render a warrantless search or seizure
11 reasonable.”). One application in which the Court has found the warrant requirement
12 inapplicable is in circumstances in which the Government faces an increased need to be able to
13 react swiftly and flexibly, or interests in public safety beyond the interests in ordinary law
14 enforcement are at stake. *See, e.g., Skinner v. Railway Labor Executives’ Ass’n*, 489 U.S. 602,
15 634 (1989) (drug testing of railroad personnel involved in train accidents). As should be
16 apparent, demonstrating that this body of law applies to a particular case requires reference to
17 specific facts.
18
19
20

21 [REDACTED TEXT]

22 (U) Beyond the warrant requirement, analysis of Plaintiffs’ Fourth Amendment claim
23 requires a fact-intensive inquiry regarding whether a particular search satisfies the Fourth
24 Amendment’s “central requirement . . . of reasonableness.” *McArthur*, 531 U.S. at 330; *see also*
25 *Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002). What is reasonable, of course, “depends on
26 all of the circumstances surrounding the search or seizure and the nature of the search or seizure
27
28

1 itself.” *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). Thus, the
2 permissibility of a particular practice “is judged by balancing its intrusion on the individual’s
3 Fourth Amendment interests against its promotion of legitimate Governmental interests.”
4 *Delaware v. Prouse*, 440 U.S. 648, 654 (1979).

5 [REDACTED TEXT]

6
7 (U) Indeed, in specifically addressing a Fourth Amendment challenge to warrantless
8 electronic surveillance, the court in *Halkin II* observed that “the focus of the proceedings would
9 necessarily be upon ‘the “reasonableness” of the search and seizure in question.’” 690 F.2d at
10 1001 (citing *Keith*, 407 U.S. at 308). “The valid claim of the state secrets privilege makes
11 consideration of that question impossible.” *Id.* Without evidence of the detailed circumstances
12 in which alleged surveillance activities were being conducted—that is, without “the essential
13 information on which the legality of executive action (in foreign intelligence surveillance)
14 turns”—the court in *Halkin II* held that “it would be inappropriate to resolve the extremely
15 difficult and important fourth amendment issue presented.” *Id.*¹⁶ This holding fully applies here.

16
17 [REDACTED TEXT]

18
19 (U) None of these issues can be decided on the limited, incomplete public record of what
20 has been disclosed about the Terrorist Surveillance Program. Any effort to determine the
21 reasonableness of allegedly warrantless foreign intelligence activities under such conditions
22 “would be tantamount to the issuance of an advisory opinion on the question.” *Halkin II*, 690
23 F.2d at 1001 (citing *Chagnon v. Bell*, 642 F.2d 1248, 1263 (D.C. Cir. 1980)). In sum, the
24

25
26
27 ¹⁶ (U) See also *Halkin II*, 690 F.2d at 1000 (“Determining the reasonableness of
28 warrantless foreign intelligence watchlisting under conditions of such informational poverty [due
to the state secrets assertion] . . . would be tantamount to the issuance of an advisory opinion on
the question.”).

1 lawfulness of the alleged activities cannot be determined without a full factual record, and that
2 record cannot be made in civil litigation without seriously compromising U.S. national security
3 interests.

4 **4. (U) Whether Alleged Surveillance Activities Are Properly Authorized**
5 **by Law Cannot be Resolved without State Secrets.**

6 (U) Finally, in addition to all of the foregoing issues that could not be litigated
7 without the disclosure of state secrets, adjudication of whether the alleged surveillance activities
8 have been conducted within lawful authority cannot be resolved without state secrets. Plaintiffs
9 allege "that the Program's surveillance has been conducted without Court orders" for several
10 years, and that it involves "the wholesale, long-term interception of customer communications
11 seen here." Pls. Prelim. Inj. Mem. at 20. Plaintiffs also seek to address whether the Government
12 certified to AT&T, pursuant to the statutory provisions on which Plaintiffs have based their
13 claims, the lawfulness of the alleged activities, *see id.* n. 23, and whether AT&T's reliance on
14 any such certification would have been reasonable. *Id.* at 21. And Plaintiffs put at issue (as a
15 general matter) those situations in which warrantless wiretapping may lawfully occur. *Id.* at 20-
16 21. Again quite clearly, Plaintiffs' allegations put at issue the factual basis of the alleged
17 activities.
18
19
20

21 [REDACTED TEXT]

22 (U) Litigation regarding Plaintiffs' claim that the President has acted in excess of his
23 authority also would require an exposition of the scope, nature, and kind of the alleged activities.
24 It is well-established that, pursuant to his authority under Article II of the Constitution as
25 Commander-in-Chief, the President's most basic constitutional duty is to protect the Nation from
26 armed attack. *See, e.g., The Prize Cases*, 67 U.S. 635, 668 (1862); *see generally Ex parte*
27 *Quirin*, 317 U.S. 1, 28 (1942). It is also well-established that the President may exercise his
28

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 statutory and constitutional authority to gather intelligence information about foreign enemies.
2 *See, e.g., Totten v. United States*, 92 U.S. 105, 106 (1876) (recognizing President's authority to
3 hire spies); *see also Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948)
4 ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has
5 available intelligence services whose reports neither are not and ought not to be published to the
6 world."); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936) (The President
7 "has his confidential sources of information. He has his agents in the form of diplomatic,
8 consular, and other officials."). And, as noted, courts have held that the President has inherent
9 constitutional authority to authorize foreign intelligence surveillance. *See supra*.

10
11 [REDACTED TEXT]

12
13 (U) CONCLUSION

14 For the foregoing reasons, the Court should:

15
16 1. Uphold the United States' assertion of the military and state secrets privilege and
17 exclude from this case the information identified in the Declarations of John D. Negroponte,
18 Director of National Intelligence of the United States, and Keith B. Alexander, Director of the
19 National Security Agency; and

20
21 2. Dismiss this action because adjudication of Plaintiffs' claims risks or requires the
22 disclosure of protected state secrets and would thereby risk or cause exceptionally grave harm to
23 the national security of the United States.
24
25
26
27
28

1 Respectfully submitted,

2 PETER D. KEISLER
3 Assistant Attorney General

4 CARL J. NICHOLS
5 Deputy Assistant Attorney General

6 DOUGLAS N. LETTER
7 Terrorism Litigation Counsel

8 JOSEPH H. HUNT
9 Director, Federal Programs Branch

10 s/ Anthony J. Coppolino
11 ANTHONY J. COPPOLINO
12 Special Litigation Counsel
13 tony.coppolino@usdoj.gov

14 s/ Andrew H. Tannenbaum
15 ANDREW H. TANNENBAUM
16 Trial Attorney
17 andrew.tannenbaum@usdoj.gov
18 U.S. Department of Justice
19 Civil Division, Federal Programs Branch
20 20 Massachusetts Avenue, NW
21 Washington, D.C. 20001
22 Phone: (202) 514-4782/(202) 514-4263
23 Fax: (202) 616-8460/(202) 616-8202

24 Attorneys for United States of America

25 DATED: May 12, 2006

26 MEMORANDUM OF THE UNITED STATES IN SUPPORT
27 OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
28 OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

CERTIFICATE OF SERVICE

I hereby certify that the foregoing **NOTICE OF MOTION AND MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT BY THE UNITED STATES OF AMERICA** will be served by means of the Court's CM/ECF system, which will send notifications of such filing to the following:

Electronic Frontier Foundation
Cindy Cohn
Lee Tien
Kurt Opsahl
Kevin S. Bankston
Corynne McSherry
James S. Tyre
545 Shotwell Street
San Francisco, CA 94110

Lerach Coughlin Stoia Geller Rudman & Robbins LLP
Reed R. Kathrein
Jeff D. Friedman
Shana E. Scarlett
100 Pine Street, Suite 2600
San Francisco, CA 94111

Traber & Voorhees
Bert Voorhees
Theresa M. Traber
128 North Fair Oaks Avenue, Suite 204
Pasadena, CA 91103

Pillsbury Winthrop Shaw Pittman LLP
Bruce A. Ericson
David L. Anderson
Patrick S. Thompson
Jacob R. Sorensen
Brian J. Wong
50 Freemont Street
PO Box 7880
San Francisco, CA 94120-7880

Sidney Austin LLP
David W. Carpenter
Bradford Berenson
Edward R. McNicholas
David L. Lawson
1501 K Street, NW
Washington, DC 20005

s/ Anthony J. Coppolino

CERTIFICATE OF SERVICE, Case No. C 06-0672-VRW

STATE OF MICHIGAN
BEFORE THE MICHIGAN PUBLIC SERVICE COMMISSION

* * * * *

In the matter of the complaint of)
AMERICAN CIVIL LIBERTIES UNION FUND)
OF MICHIGAN against **AT&T MICHIGAN.** and)
VERIZON NORTH, INC)

Case No. U-14985

RULING SUSPENDING COMPLAINT

1. During the course of the September 29, 2006 motion hearing, the issue of whether the ACLU's complaint met the filing requirements of MCL 484.2203(7) was raised.
2. Under MCL 484.2203(7) a telecommunications complaint that fails to contain all the "information, testimony, [and] exhibits . . . on which the person intends to rely . . . shall be dismissed or suspended pending the receipt . . . of the required information.
3. The complaint filed by the ACLU fails to contain any pre-filed testimony, as required by MCL 484.2203(7) and Administrative Rule 460.17331.

ORDER

It is ordered that, pursuant to MCL 484.2203(7), the Complaint is suspended.

STATE OFFICE OF ADMINISTRATIVE
HEARINGS AND RULES
For the Michigan Public Service Commission

Mark D.
Eyster

Mark D. Eyster
Administrative Law Judge

Digitally signed by Mark D. Eyster
DN: cn=Mark D. Eyster, c=US,
email=mdeyste@michigan.gov
Date: 2006.10.18 14:20:09 -04'00'

October 19, 2006
dmp