

EXHIBIT 17

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

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

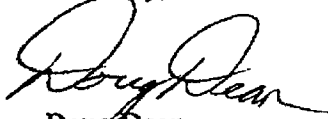
www.dora.state.co.us/puc
Permit and Insurance (Outside Denver) 1-800-888-0170
TTY Users 711 (Relay Colorado)
Consumer Affairs 303-894-2070

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 cursive script, appearing to read "Doug Dean".

Doug Dean
Director

EXHIBIT 18



STATE OF DELAWARE
PUBLIC SERVICE COMMISSION
861 SILVER LAKE BOULEVARD
CANNON BUILDING, SUITE 100
DOVER, DELAWARE 19904

TELEPHONE: (302) 739 - 4247
FAX: (302) 739 - 4849

*copied to K Henry
Benson
McNicholas
R. Young*

July 12, 2006

Julia M. Graff, Esquire
American Civil Liberties
Union of Delaware
100 West 10th Street
Suite 309
Wilmington, Delaware 19801

Re: In the Matter of the Request of Ten
Customers to Initiate an Investigation
Into Whether Verizon Delaware Inc. and
AT&T Communications of Delaware LLC,
Have Improperly Shared Telephone Records
(Filed May 25, 2006) -
PSC Docket No. 06-179

Dear Ms. Graff:

Enclosed are two (2) Certified Copies of Commission Order No. 6965
in the above-captioned matter, which are self-explanatory.

Very truly yours,

Karen J. Nickerson
Secretary

KJN/njs
Enclosures: 2
Certified Mail #000675487216
cc: Gary A. Myers, Esq. (w/encl)
David W. Carpenter, Esq. (w/encl) ✓
Anthony E. Gay, Esq. (w/enc)
Leigh A. Hyer, Esq. (w/encl)
G. Arthur Padmore (w/encl)

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

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).

pending throughout the country, challenging carriers' alleged 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.

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).


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

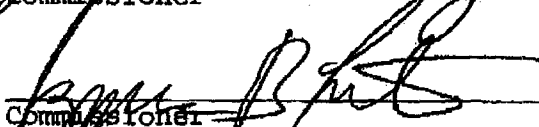
1. That proceedings in this matter, resulting from the petition or complaint filed by Helen K. Foss, Enno Krebbers, Phyllis Levitt, Lawrence Hamermesh, Marion Hamermesh, Judith Mellen, Joy Mulholland, Gilbert Sloan, Sonia Sloan, and Serena Williams on May 26, 2006, are hereby held in abeyance for a period 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.

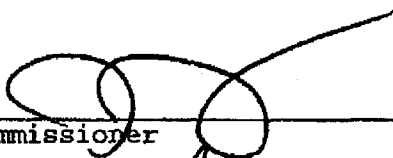
BY ORDER OF THE COMMISSION:


Chair

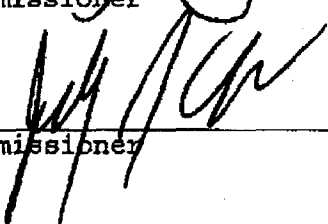

Commissioner


Commissioner

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



Commissioner



Commissioner

ATTEST:



Secretary

EXHIBIT 19

[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 Upihegrove (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.

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

EXHIBIT 20

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

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

UNITED STATES DISTRICT COURT
 FOR THE DISTRICT OF NEW JERSEY

THE UNITED STATES OF AMERICA,)
)
 Plaintiff,)
)
 v.)
)
 ZULIMA V. FARBER, in her official capacity as)
 Attorney General of the State of New Jersey;)
 CATHLEEN O'DONNELL, in her official)
 capacity as Deputy Attorney General of the State)
 of New Jersey; KIMBERLY S. RICKETTS, in)
 her official capacity as Director of the New Jersey)
 Division of Consumer Affairs; AT&T CORP.;)
 VERIZON COMMUNICATIONS INC; QWEST)
 COMMUNICATIONS INTERNATIONAL, INC.;)
 SPRINT NEXTEL CORPORATION; and)
 CINGULAR WIRELESS LLC,)
)
 Defendants.)

CIVIL ACTION NO.:
 COMPLAINT

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

INTRODUCTION

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

JURISDICTION AND VENUE

2. The Court has jurisdiction pursuant to 28 U.S.C. §§ 1331, 1345.
3. Venue lies in the District of New Jersey pursuant to 28 U.S.C. § 1391(b)(1) and (2).

PARTIES

4. Plaintiff is the United States of America, suing on its own behalf.
5. Defendant Zulima V. Farber is the Attorney General for the State of New Jersey, and maintains her offices in Mercer County. She is being sued in her official capacity.
6. Defendant Cathleen O'Donnell is the Deputy Attorney General for the State of New Jersey, and maintains her offices in Mercer County. She is being sued in her official capacity.
7. Defendant Kimberly S. Ricketts is the Director of the New Jersey Division of Consumer Affairs. She is being sued in her official capacity. Defendants Zulima V. Farber, Cathleen O'Donnell, and Kimberly S. Ricketts are referred to as the "State Defendants."
8. Defendant AT&T Corp. is a corporation incorporated in the state of New York with its principal place of business in Somerset County, New Jersey, and that has received a subpoena in New Jersey.
9. Defendant Verizon Communications Inc. is a corporation incorporated in the state of Delaware with its principal place of business in the state of New York, that has offices in Somerset County, New Jersey, and that has received a subpoena in New Jersey.
10. Defendant Qwest Communications International, Inc. is a corporation incorporated in the state of Delaware with its principal place of business in the state of Colorado, and that has received a subpoena in New Jersey.
11. Defendant Sprint Nextel Corporation is a corporation incorporated in the state of New Jersey with its principal place of business in the state of Virginia, and that has received a subpoena in New Jersey.
12. Defendant Cingular Wireless LLC is a corporation incorporated in the state of Delaware with its principal place of business in Georgia, and that has received a subpoena in

New Jersey.

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

STATEMENT OF THE CLAIM

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

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

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

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

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

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

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

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

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

A person may have access to classified information provided that:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

32. Director Negroponete 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.” Negroponete 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.” Negroponete Decl. ¶ 12; see Alexander Decl. ¶ 8. The assertion of the privilege encompasses “allegations about NSA’s purported involvement with AT&T.” Negroponete Decl. ¶ 12; Alexander Decl. ¶ 8. Director Negroponete 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

EXHIBIT 21



U. S. Department of Justice

Civil Division

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

The Honorable Zulima V. Farber
Page 2

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."

The Honorable Zulima V. Farber
Page 3

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.

The Honorable Zulima V. Farber
Page 4

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).

The Honorable Zulima V. Farber
Page 5

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," Negroponde 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 Negroponde 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." Negroponde Decl. ¶12; see also Alexander Decl. ¶8. As DNI Negroponde 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." Negroponde 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 Honorable Zulima V. Farber
Page 6

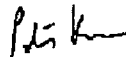
the DNI's authority and the Act of Congress conferring that authority. More broadly, the subpoenas involve an improper effort to use state law to regulate or oversee federal functions, and implicate federal immunity under the Supremacy Clause.

* * *

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

EXHIBIT 22



U. S. Department of Justice

Civil Division

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

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

Christina 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.

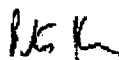
As noted in our Complaint and letter to Attorney General Farber concerning those issues, the subpoenas infringe upon federal operations, are contrary to federal law, and are invalid under the Supremacy Clause of the United States Constitution. Responding to the subpoenas – including by disclosing whether 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,



Peter D. Keisler
Assistant Attorney General

Attachments

EXHIBIT 23

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

WASHINGTON, DC 20511

July 11, 2006

VIA FACSIMILE (202) 736-8711
AND FIRST CLASS MAIL

Edward R. McNicholas
Sidley Austin LLP
1501 K Street, N.W.
Washington, D.C. 20005

Dear Mr. McNicholas,

We understand that subpoenas duces tecum issued by two Missouri Public Service Commissioners were served upon TCG Kansas City, Inc., TCG St. Louis Holdings, Inc., SBC Long Distance, L.L.C., SBC Advanced Solutions, Inc., Southwestern Bell Telephone, L.P., and AT&T Communications of the Southwest, Inc. on June 19, 2006, and June 22, 2006. The subpoenas seek materials and information allegedly disclosed to the National Security Agency, and materials and information related to the alleged release of customer proprietary information.

Compliance with the subpoenas by these entities would place them in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without harming national security. Further enforcement of the 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. Responding to the subpoenas, including disclosing whether, or to what extent, any responsive materials or information exist, would violate various specific provisions of federal statutes and Executive Orders. Further, the Director of National Intelligence recently asserted the state secrets privilege with respect to the very same topics and types of information sought by the subpoenas. This underscores that any such information cannot be disclosed. Finally, the United States recently filed a lawsuit against the Attorney General and other officials of the State of New Jersey, and several telecommunication carriers, seeking a declaration that the defendant state officials do not have the authority to enforce similar subpoenas, and that the defendant telecommunication carriers cannot respond to the subpoenas. For these reasons, please be advised that it is our position that enforcing compliance with, or responding to, the subpoenas would be inconsistent with, and preempted by, federal law.

Please do not hesitate to contact me or Michael Castelli of my office should you have any questions in this regard.

Sincerely,



Benjamin A. Powell
General Counsel

EXHIBIT 24

**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

I. 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 the these Subpoenas would be invalid under, preempted by, and inconsistent with the Supremacy Clause of the United States Constitution, Art. VI, Cl. 2, federal law, and the Federal Government's exclusive control over foreign intelligence gathering activities, national security, the conduct of foreign affairs, and the conduct of military affairs.

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

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

EXHIBIT 25

**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. Ill.), 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 Negroponete 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 Negroponete 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.” Negroponete Decl. ¶ 11; see Alexander Decl. ¶¶ 7-8. In other words, the state secrets privilege covers precisely the same types of information that the State Defendants seek from Verizon.

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

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

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

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

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

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

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

31. The Order demands that responses be submitted by Verizon on or before August 21, 2006. Exhibit D at 4. Defendants issued this Order notwithstanding being advised by the Department of Justice on July 28, 2006, that the MPUC’s attempts to require telecommunication carriers to provide information would be inconsistent with, and preempted by, federal law. *See* Exhibit C. Indeed, a comprehensive body of federal law governs the field of foreign intelligence gathering and bars any unauthorized disclosures as contemplated by this Order, thereby preempting state law, including: (i) Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note; (ii) section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1); and (iii) 18 U.S.C. § 798(a).

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

32. The State Defendants’ attempts to seek or obtain the information requested in the August 9, 2006 Order, as well as any related information, are fundamentally inconsistent with and preempted by the Federal Government’s exclusive control over all foreign intelligence gathering activities. In addition, no federal law authorizes the State Defendants to obtain the information they seek.

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

Executive Order No. 13292.

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

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

36. The United States has a strong and compelling interest in preventing the disclosure of sensitive and classified information. The United States has a strong and compelling interest in preventing terrorists from learning about the methods and operations of terrorist surveillance activities being undertaken or not being undertaken by the United States.

37. As a result of the Constitution, federal laws, applicable privileges, and the United States' interest in preventing the unauthorized disclosure of sensitive or classified information, Verizon will be unable to confirm or deny their involvement, if any, in intelligence activities of the United States.

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

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

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

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

or any other related information, are invalid under, and preempted by, the Supremacy Clause of the United States Constitution, Art. VI, Cl. 2, federal law, and the Federal Government's exclusive control over foreign intelligence gathering activities, national security, the conduct of foreign affairs, and the conduct of military affairs.

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

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

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

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

PRAYER FOR RELIEF

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

1. That this Court enter a declaratory judgment pursuant to 28 U.S.C. § 2201(a), that the State Defendants may not enforce the Order or otherwise seek information pertaining to alleged foreign intelligence functions of the federal government and that Verizon may not provide such information, because any attempt to obtain or disclose such information would be invalid under, preempted by, and inconsistent with the Supremacy Clause of the United States Constitution, Art. VI, Cl. 2, federal law, and the Federal Government's exclusive control over foreign intelligence gathering activities, national security, the conduct of foreign affairs, and the conduct

of military affairs.

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

Dated: August 21, 2006

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

PAULA D. SILSBY
United States Attorney

CARL J. NICHOLS
Deputy Assistant Attorney General

DOUGLAS LETTER
Terrorism Litigation Counsel

ARTHUR R. GOLDBERG
Assistant Director, Federal Programs Branch

/s/ Alexander K. Haas

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

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

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

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

I, Keith B. Alexander, declare as follows:

INTRODUCTION

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

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

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

THE NATIONAL SECURITY AGENCY

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

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

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

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

INFORMATION SUBJECT TO CLAIMS OF PRIVILEGE

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

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

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

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

CONCLUSION

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

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

DATE: 30 June 86



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

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

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

**DECLARATION OF JOHN D. NEGROPONTE,
DIRECTOR OF NATIONAL INTELLIGENCE**

I, John D. Negroponte, declare as follows:

INTRODUCTION

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

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

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

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

THE DIRECTOR OF NATIONAL INTELLIGENCE

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

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

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

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

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

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

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

ASSERTION OF THE STATE SECRETS PRIVILEGE

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

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

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

INFORMATION SUBJECT TO CLAIMS OF PRIVILEGE

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

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

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

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

CONCLUSION

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

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

DATE: 6/30/06


JOHN D. NEGROPONTE
Director of National Intelligence



U. S. Department of Justice

Civil Division

Assistant Attorney General

Washington, D.C. 20530

July 28, 2006

VIA FACSIMILE AND FEDERAL EXPRESS

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

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

Dear Chairman Adams and Commissioner Reishus:

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

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

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

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

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

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

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

to allegedly provide customer records to the NSA. See Complainant's 1st Data Request to Verizon of May 9, 2006 (incorporating January 20, 2006 requests from Representative Conners) & Complainant's 2d Data Request to Verizon of May 15, 2006. Thus, the requests seek information, including *inter alia*: whether Verizon has "ever given the government access to any . . . hardware or software used to deliver communications services in response to a request that was not compelled" by certain designated processes; whether Verizon "ever turned over customer records to the federal government in response to a request that was not compelled" by certain designated processes; "how many call records in total has Verizon provided to NSA;" "how many are its Maine customers' records, and how many of those are records of those customers' intrastate calls;" and "[b]y what processes does Verizon provide NSA its customers' call records." See *id.* Should the MPUC open an investigation and complainants refile these requests, or if the MPUC itself seeks its own similar discovery, such an exertion of regulatory authority² with respect to the nation's foreign-intelligence gathering would seek to use state regulatory authority to intrude upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with federal prerogatives. That effort is fundamentally inconsistent with the Supremacy Clause. *McCulloch*, 17 U.S. at 326-27 (1819) ("[T]he states have no power . . . to retard, impede, burden, or in any manner control, the operations of the constitutional laws enacted by Congress to carry into execution the power vested in the general government."); see also *Leslie Miller, Inc. v. Arkansas*, 352 U.S. 187 (1956).

The Supreme Court's decision in *American Insurance Ass'n v. Garamendi*, 539 U.S. 396 (2003), is the most recent precedent that demonstrates that such state-law based information requests are preempted by federal law. In *Garamendi*, the Supreme Court held invalid subpoenas issued by the State of California to insurance carriers pursuant to a California statute that required those carriers to disclose all policies sold in Europe between 1920 and 1945, concluding that California's effort to impose such disclosure obligations interfered with the President's conduct of foreign affairs. Here, such requests for information would seek the disclosure of information that infringes on the Federal Government's intelligence gathering authority and on the Federal Government's role in protecting the national security at a time when we face terrorist threats to the United States homeland; any such requests for information, just like the subpoenas at issue in *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 Any such information request would likely fall under MPUC Rules of Procedure 821 or 822 regarding data requests or Rules of Procedure 730 and 731 regarding subpoena practice.

2. Responding to such requests for information, including merely disclosing whether or to what extent any responsive materials exist, would also violate various federal statutes and Executive Orders. Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note, provides: “[N]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of persons employed by such agency.”³ *Ibid.* (emphasis added). Similarly, section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1), confers upon the Director of National Intelligence (“DNI”) the authority and responsibility to “protect intelligence sources and methods from unauthorized disclosure.” *Ibid.*⁴ (As set forth below, the DNI has determined that disclosure of the types of information sought by the information requests would harm national security.)

Several Executive Orders promulgated pursuant to the foregoing constitutional and statutory authority govern access to and handling of national security information. Of particular importance here, Executive Order No. 12958, 60 Fed. Reg. 19825 (April 17, 1995), as amended by Executive Order No. 13292, 68 Fed. Reg. 15315 (March 25, 2003), prescribes a comprehensive system for classifying, safeguarding, and declassifying national security information. It provides that a person may have access to classified information only where “a favorable determination of eligibility for access has been made by an agency head or the agency head’s designee”; “the person has signed an approved nondisclosure agreement”; and “the person

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

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

has a need-to-know the information." That Executive Order further states that "Classified information shall remain under the control of the originating agency or its successor in function." Exec. Order No. 13292, Sec. 4.1(c). Exec. Order No. 13292, Sec. 4.1(a).

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

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

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

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

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

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

* * *

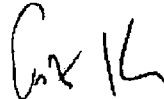
⁵ Although Judge Walker did not grant the government's motion to dismiss on state secrets grounds at this stage in *Hepting*, he declined to permit discovery on communications records allegations. The United States respectfully disagrees with his decision not to dismiss the case on state secrets ground;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

Chairman Kurt Adams
Commissioner Sharon M. Reishus
Page 7

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

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

Sincerely,



Peter D. Keisler
Assistant Attorney General

Enclosures

cc: ME Docket 2006-274 service list

STATE OF MAINE
PUBLIC UTILITIES COMMISSION

Docket No. 2006-274

August 9, 2006

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

ORDER

ADAMS, Chairman; REISHUS, Commissioner

I. SUMMARY

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

II. BACKGROUND

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

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

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

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

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

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

1. Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records from any of its businesses, or any call data from those records.
2. None of these companies – wireless or wireline – provided customer records or call data.
3. Verizon's wireless and wireline companies did not provide to NSA customer records or call data, local or otherwise.
4. Verizon will provide customer information to a government agency only where authorized by law for appropriately-defined and focused purposes.
5. When information is provided, Verizon seeks to ensure it is properly used for that purpose and is subject to appropriate safeguards against improper use.
6. Verizon does not, and will not, provide any government agency unfettered access to its customer records or provide information to the government under circumstances that would allow a fishing expedition.
7. Verizon acquired MCI, and Verizon is ensuring that Verizon's policies are implemented at that entity and that all its activities fully comply with law.

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

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

III. DISCUSSION AND DECISION

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

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

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

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

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

IV. CONCLUSION

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

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

BY ORDER OF THE COMMISSION

Dennis L. Keschl
Acting Administrative Director

COMMISSIONERS VOTING FOR:

Adams
Reishus

EXHIBIT 26

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.” Negroponete 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


EXHIBIT 27

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.)

CLERK
BY _____ DEPUTY CLERK 

CIVIL ACTION NO.:
COMPLAINT 2:06-cv-188

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

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,

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

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

- 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."

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).

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

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

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.

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

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

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

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

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.

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

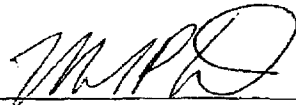
DOUGLAS LETTER
Terrorism Litigation Counsel

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



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

EXHIBIT 28



U. S. Department of Justice

Civil Division

Assistant Attorney General

Washington, D.C. 20530

July 28, 2006

VIA FACSIMILE AND FEDERAL EXPRESS

Chairman James Volz
Board Member David C. Coen
Board Member John D. Burke
Vermont Public Service Board
112 State Street
Drawer 20
Montpelier, Vermont 05620

Re: Docket Nos. 7183, 7192, & 7193; July 12, 2006, Procedural Order

Dear Chairman Volz and Board Members Coen and Burke:

I write in response to the July 12, 2006, Procedural Order ("Procedural Order") issued by the Vermont Public Service Board ("VPSB") inviting the United States "to intervene in this proceeding in order to protect the interests of the United States." See Procedural Order at 5, enclosed hereto. I also understand that motions to dismiss these proceedings are pending before the VPSB. The United States appreciates the opportunity to provide its views to the VPSB. Please note, however, that our willingness to provide our views is not, and should not be deemed, either as a formal intervention in this matter or the submission of the United States to the jurisdiction of the State of Vermont.

It is my understanding that the Vermont Department of Public Services ("DPS") sent information requests to Verizon New England, Inc. ("Verizon") and AT&T Communications of New England, Inc. ("AT&T") (collectively the "carriers") in May 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 May 17 from Commissioner David O'Brien to Bruce P. Beausejour and Pamela Porell at requests 1-16, ("Document Requests") (a copy of this letter is enclosed hereto).

It is the position of the United States that compliance with the DPS Document Requests, and any similar discovery propounded in this VPSB proceeding, would place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or

Chairman James Volz
Board Member David C. Coen
Board Member John D. Burke
Page 2

denied without harming national security, and that enforcing compliance with such requests for information would be inconsistent with, and preempted by, federal law.

I note that the Procedural Order recognizes the "incompatible state and federal obligations" on the carriers and expresses an interest in avoiding an imposition of such obligations. See Procedural Order at 3. Toward that end, this letter outlines the basic reasons why, in our view, the Document Requests that led to these proceedings, and any similar discovery propounded in this proceeding, are preempted by federal law and that compliance with such requests would violate federal law. In similar situations in both New Jersey and Missouri, the United States has acted to protect its sovereign interests by filing lawsuits to preclude the enforcement of subpoenas that seek disclosure of similar information. We sincerely hope that, in light of governing law and the national security concerns implicated by the requests for information, you will dismiss these petitions 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 requests for information at issue here interfere with and seek the disclosure of information regarding the Nation's foreign-intelligence gathering. But it has been clear since at least *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316, 4 L.Ed. 579 (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 requests for information demand that the carriers produce information regarding specified categories of communications between each carrier and the NSA since January 1, 2001, including *inter alia* "categories of information [] 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;" whether the carrier "disclosed or delivered to any other state or federal agency the phone call records of any [] customer in Vermont since January 1, 2001;" "the format in which the information was provided;" "the reporting interval for the provision of such information;" "how many of [the carrier's] Vermont customers have had their calling records disclosed or turned over to the NSA or any other governmental entity, on an agency-by-agency basis, since the inception of the disclosures;" "whether the disclosures of [the

Chairman James Volz
Board Member David C. Coen
Board Member John D. Burke
Page 3

carrier's] Vermont customer call information to the NSA and/or any state or federal agency is ongoing;" "the number of occasions that Verizon has made such disclosure;" whether the carrier is "disclosing records for any communications services other than telephone calling records;" whether "any such disclosures were made by [the carrier] [] voluntarily upon request of a governmental agency . . . [or] in response to an exercise of governmental authority . . . [and what] specific authority [the carrier] relied upon;" and 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 an agency of the federal government." See Document Requests, ¶¶ 1-16. In seeking to exert regulatory authority¹ with respect to the nation's foreign-intelligence gathering, the DPS has thus sought to use state regulatory authority to intrude upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with federal prerogatives. That effort is fundamentally inconsistent with the Supremacy Clause. *McCulloch*, 17 U.S. at 326-27 ("[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 information requests are preempted by federal law. In *Garamendi*, the Supreme Court held invalid subpoenas issued by the State of California to insurance carriers pursuant to a California statute that required those carriers to disclose all policies sold in Europe between 1920 and 1945, concluding that California's effort to impose such disclosure obligations interfered with the President's conduct of foreign affairs. Here, the requests for information 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 requests for information, 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").

¹ The information request makes clear that the DPS issued the request "[p]ursuant to its statutory authority under 30 V.S.A. § 206." Likewise, any independent request for information or discovery by the VPSB would be pursuant to similar state law. See 30 V.S.A. § 18. *Accord* Rules and General Orders of the VPSB § 2.214.

Chairman James Volz
Board Member David C. Coen
Board Member John D. Burke
Page 4

2. Responding to the requests for information, including merely disclosing whether or to what extent any responsive materials exist, would also violate various federal statutes and Executive Orders. Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note, provides: “[N]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of persons employed by such agency.”² *Ibid.* (emphasis added). Similarly, section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1), confers upon the Director of National Intelligence (“DNI”) the authority and responsibility to “protect intelligence sources and methods from unauthorized disclosure.” *Ibid.*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.)

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

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*, 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 James Volz
Board Member David C. Coen
Board Member John D. Burke
Page 5

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 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).

Vermont 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 any Vermont agency's requests for information seek to compel disclosure of such information to state officials, 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 sought by these requests for information, underscores that compliance with the requests for information 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,

Chairman James Volz
Board Member David C. Coen
Board Member John D. Burke
Page 6

that it is gathering information from a particular source, or that it has gathered information on a particular person, such intelligence-gathering activities would be compromised and foreign adversaries such as al Qaeda and affiliated terrorist organizations could use such information to avoid detection." See Unclassified Declaration of John D. Negroponte in *Terkel* ("Negroponte Decl.") ¶ 12, enclosed hereto. Furthermore, "[e]ven confirming that a certain intelligence activity or relationship does *not* exist, either in general or with respect to specific targets or channels, would cause harm to the national security because alerting our adversaries to channels or individuals that are not under surveillance could likewise help them avoid detection." *Id.*

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 sought from the carriers by Vermont officials.

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*, Slip. Op. at 32, enclosed hereto. In seeking to have telecommunication carriers confirm or deny similar information, the requests at issue here thus seek the very type of disclosures deemed inimical to the national security in *Terkel* by both the DNI and Judge Kennelly.⁴

* * *

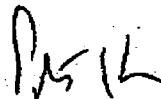
⁴ In another pending case raising similar issues, *Hepting v. AT&T Corp.*, No. 06-0672-VRW (N.D. Cal.), although the Court did not grant the government's motion to dismiss at this stage, it declined to permit discovery on communications records allegations. The United States respectfully disagrees with his decision not to dismiss the case on state secrets ground; Judge Walker himself certified his order for immediate appeal, and the United States will appeal. In any event, however, a *federal court's* authority regarding the assertion of state secrets in no way whatsoever provides authority for a state administrative body, otherwise without authority under the Constitution in this area, to order the release of classified information or otherwise interfere with alleged federal government operations.

Chairman James Volz
Board Member David C. Coen
Board Member John D. Burke
Page 7

Accordingly, for the reasons outlined above, it is the United States' position that the requests for information and the application of state law they embody are inconsistent with and preempted under the Supremacy Clause, and that compliance with these requests, or any similar discovery propounded by the VPSB, 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

Enclosures

EXHIBIT 29



U. S. Department of Justice

Civil Division

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 Negroonte 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. Negroonte in *Terkel* (“Negroonte 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 Martincz
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

EXHIBIT 30



U. S. Department of Justice

Civil Division

Assistant Attorney General

Washington, D.C. 20530

October 13, 2006

VIA FACSIMILE AND FEDERAL EXPRESS

Nebraska Public Service Commission
1200 N Street, Suite 300
Lincoln, Nebraska 68508

Attention: Commissioner Frank E. Landis, Jr.
Commissioner Anne C. Boyle
Commissioner Lowell C. Johnson
Commissioner Rod Johnson
Commissioner Gerald L. Vap

Re: Docket Nos. FC-1322 & FC-1323; Miller/ACLU v AT&T; Miller/ACLU v. Verizon

Dear Commissioners Landis, Boyle, Johnson, Johnson, and Vap:

I write with regard to the above-referenced dockets pending before the Nebraska Public Service Commission ("NPSC"). I understand that motions to dismiss these proceedings are currently pending before the NPSC, and the United States of America would like to take the opportunity to provide its views to the NPSC 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 Nebraska.

The American Civil Liberties Union Nebraska Foundation ("ACLU") initiated these proceedings against AT&T 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 24, 2006 from ACLU to NPSC (the "ACLU Letter"), attached hereto. In particular, the ACLU requests that an investigation be opened, so that the NPSC can attempt to ascertain the truth of the allegations in the news reports over the purported United States' foreign intelligence gathering program, which the ACLU asserts may have violated Nebraska law.

It is the position of the United States that, in light of the allegations on the face of the ACLU Letter and complaints, the NPSC 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

Commissioners Landis, Boyle, Johnson, Johnson and Vap

October 13, 2006

Page 2

dismiss. Notably, the NPSC would be unable to engage in any discovery propounded in this NPSC 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 NPSC 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, Connecticut, and Vermont the United States has acted to protect its sovereign interests by filing lawsuits to preclude the enforcement of state administrative subpoenas or 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 Nebraska state law, through the NPSC, to investigate the nature of, interfere with, and seek the disclosure of information regarding the Nation's foreign-intelligence gathering activities, and specifically to inquire into whether the carriers have aided in a purported NSA intelligence program, *see* ACLU Letter at 1. 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 Federal 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 authority 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 federal prerogatives.¹ That effort is fundamentally inconsistent with the Supremacy Clause.

¹ The ACLU Complaint makes clear that it is founded on numerous provisions of the "State of Nebraska code." *See* ACLU Complaint against AT&T at 2-3, attached hereto (citing Nebraska code sections).

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 follow 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 NPSC to undertake – an investigation into alleged foreign-intelligence gathering operations of the United States.

2. If the NPSC does not dismiss this action and goes on to conduct an investigation, it will, through the use of its discovery processes, 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*, 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*,

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 that would be sought in the NPSC’s discovery process 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 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).

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.

No Nebraska state official (nor any member of the ACLU) has 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 NPSC 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 that would be sought in this case. In particular in *Terkel*, Director Negroonte 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. Negroonte in *Terkel* ("Negroonte 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.*

In light of the exceptionally grave damage to national security that could result from any such information, Director Negroonte 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 Nebraska 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 NPSC exert its investigatory process under Nebraska law over the carriers, the NPSC 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 in the Eastern District of Michigan held that "the state secrets privilege applies to Plaintiffs' data-mining claim," *i.e.*, a claim based on 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.

* * *

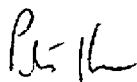
Accordingly, for the reasons outlined above, it is the United States' position that the NPSC has no authority in this area to investigate the alleged foreign-intelligence gathering functions of the United States and that the Supremacy Clause preempts any attempt to use state law to conduct such investigations. 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 NPSC 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.

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; Chief Judge Walker himself certified the 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.

Commissioners Landis, Boyle, Johnson, Johnson and Vap
October 13, 2006
Page 7

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: Andrew Pollock, Executive Director Nebraska PSC (by mail)
Loel P. Brooks, Esq. (by mail)
David W. Carpenter, Esq. (by mail)
Amy Miller, Esq. (by mail)