BEFORE THE PUBLIC UTILITY COMMISSION

OF OREGON

UM 1265

AMERICAN CIVIL LIBERTIES UNION OF OREGON, INC. and AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF OREGON, INC., Complainants, v. VERIZON NORTHWEST, INC., and QWEST CORPORATION, Defendants.	DECLARATION OF LAURA CALDERA TAYLOR IN SUPPORT OF COMPLAINANTS' REQUEST FOR JUDICIAL NOTICE REGARDING OPPOSITION TO VERIZON'S MOTION TO DISMISS

I, Laura Caldera Taylor, do hereby declare:

1. I am an attorney with Garvey Schubert Barer, counsel of record for Complainants in this matter.

2. Attached hereto as Exhibit No. 1 is a true and correct copy of the Vermont Order on Motion to Dismiss, dated September 18, 2006.

3. Attached hereto as Exhibit No. 2 is a true and correct copy of *2004 Ore. PUC LEXIS 10.*

4. Attached hereto as Exhibit No. 3 is a true and correct copy of a May 3,

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

2006 letter from Andie Arthurholtz, Nevada Compliance Investigator to Gary Peek, Executive Director, ACLU of Nevada.

5. Attached hereto as Exhibit No. 4 is a true and correct copy of a May 3, 2006 letter from Andie Arthurholtz, Nevada Compliance Investigator to Gary Peek, Executive Director, ACLU of Nevada.

6. Attached hereto as Exhibit No. 5 is a true and correct copy of Vermont Orders Opening Investigation of Verizon, dated June 27, 2006.

7. Attached hereto as Exhibit No. 6 is a true and correct copy of Vermont Orders Opening Investigation and Notice of Prehearing Conference regarding AT&T, dated June 29, 2006.

I hereby declare that the above statement is true to the best of my knowledge and belief, and that I understand it is made for use as evidence in court and is subject to penalty for perjury.

DATED this 21 day of October, 2006.

Laura Caldera Taylor

LAURA CALDERA TAYLOR

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

CERTIFICATE OF SERVICE

I hereby certify that the foregoing DECLARATION OF LAURA CALDERA TAYLOR IN SUPPORT OF COMPLAINANTS' REQUEST FOR JUDICIAL NOTICE REGARDING OPPOSITION TO QWEST'S MOTION TO DISMISS was served on:

Alex M. Duarte
Corporate Counsel
Qwest Corporation
421 SW Oak Street, Ste. 810
Portland, OR 97204
E-Mail: alex.duarte@qwest.com

Heather Zachary
Wilmer Cutler Pickering
Hale and Dorr LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20009
E-Mail: heather.zachary@wilmerhale.com

Gregory Romano
General Counsel
Verizon Corporate Services
MC WA0105RA
1800 41st Street
Everett, WA 98201
E-mail: Gregory.m.romano@verizon.com

Renee Willer
Manager Regulatory &
Government Affairs
Verizon Corporate Services
MC: OR030156
20575 NW Von Neumann Dr., Ste 150
Hillsboro, OR 97006-4771
E-mail: renee.willer@verizon.com

Citizens' Utility Board of Oregon
OPUC Dockets
610 SW Broadway, Ste. 308
Portland, OR 97205
E-Mail: dockets@oregoncub.org

Jason Eisdorfer
Energy Program Director
Citizens' Utility Board of Oregon
610 SW Broadway, Ste. 308
Portland, OR 97205
E-Mail: Jason@oregoncub.org

by mailing to them a copy of the original thereof, contained in sealed envelopes, addressed as above set forth, with postage prepaid, and deposited in the mail in Portland, Oregon, on October 27, 2006.

Laura Caldera Taylor
Of Attorneys for Complainants

PDX_DOCS:381672.1 [30186-00114]

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

STATE OF VERMONT
PUBLIC SERVICE BOARD

Docket No. 7193

Petition of Vermont Department of Public)
Service for an investigation into alleged)
unlawful customer records disclosure by AT&T)
Communications of New England, Inc.)

Order entered: 9/18/2006

ORDER ON MOTION TO DISMISS

SUMMARY

This Order denies AT&T's motion to dismiss. We have jurisdiction under state law to proceed in this matter, and it has not been shown that federal law preempts that jurisdiction. Nothwithstanding the many bases upon which AT&T asserts that the claims here are preempted by federal law, we conclude that the Department of Public Service may still be able to adduce facts that sustain at least some of its claims. We recognize that discovery in this case may be limited, but we allow the Department to seek to prove its case by whatever unprivileged evidence it can glean from discovery of AT&T and from whatever other reliable sources that may develop.

Based on the record before us, we conclude that the state secrets privilege does not apply here, largely because it has not been properly claimed, but also because it would not apply to all claims. We also conclude that dismissal is not required by the National Security Agency statute, the Foreign Intelligence Surveillance Act, the statutes and rules regarding classified information, or the Intelligence Reform and Terrorism Prevention Act of 2004.

TABLE OF CONTENTS

I. BACKGROUND

The Petition

This docket was commenced to examine whether AT&T Communications of New England, Inc. ("AT&T") violated Vermont utility standards by disclosing customer record information to the National Security Agency ("NSA") or other federal or state agencies[1] ("NSA Customer Records Program"). It was initiated by petition of the Vermont Department of Public Service ("Department") filed on June 21, 2006. The petition reported that the Department had sought information from AT&T, but that AT&T's response did "not even attempt to answer" the questions posed by the Department. The petition alleges that this has obstructed the Department in its statutory duties and that any disclosures to the NSA, if they have occurred, would have violated state and federal laws. The petition concludes by requesting that penalties be imposed on AT&T for its failure to adequately respond and any further relief that the Board deems proper.

Attached to the petition was a copy of the Department's information request, dated May 17, 2006, and a brief response letter from AT&T, dated May 25, 2006. In AT&T's letter, it asserts that it "does not give customer information to law enforcement authorities or government agencies without legal authorization" and that any release of information to law enforcement officials, occurs "strictly within the law." The letter also states that "matters of national security . . . must be addressed on a national basis."

There are no allegations that AT&T was coerced into participating in the NSA Customer Records Program. It has been reported that one major Bell company, Qwest, elected not to participate.[2] The Department's discovery request and petition have raised the following questions of fact:

1. Whether AT&T participated in the NSA Customer Records Program.

---

1. The Department also sought information from AT&T regarding similar disclosures to any other federal or state agency. In the text below , "NSA Customer Records Program" should be read as including disclosures to and activity by any state or federal agency, including but not limited to the NSA.

2. According to counsel for Qwest's former Chief Executive Officer Joseph Nacchio, the government approached Mr. Nacchio several times between the fall of 2001 and the summer of 2002 to request its customer telephone records, but because the government failed to cite any legal authorization in support of its demands, Mr. Nacchio refused the requests. *See* John O'Neil, *Qwest's Refusal of N.S.A. Query Is Explained*, N.Y. Times, May 12, 2006. Quoted in *Terkel v. AT&T Corp.*, ___ F.Supp. ___, 2006 WL 2088202, slip op. at 23 (N.D.Ill. July 25, 2006) (hereafter "*Terkel*").

2. If AT&T did participate:
   a. What kinds of information were provided, for how many customers, in what form and when?
   b. Did AT&T modify its equipment in Vermont to participate?
   c. Did AT&T act voluntarily? Did it act in response to an exercise of governmental authority?
   d. Did AT&T receive compensation? If so, how much? How much is attributable to Vermont?
3. What is AT&T's policy for responding to state law enforcement requests for call records of Vermont customers?
4. What records, if any, does AT&T keep regarding requests by law enforcement for call records of Vermont customers?

The NSA also operates a program that intercepts the contents of certain communications where one party to the communication is outside the United States and where the government has a reasonable basis to conclude that one party to the communication has a relationship with al Qaeda.[3] One federal court has held that this content interception program violates the Administrative Procedures Act, the Separation of Powers Doctrine, the First and Fourteenth Amendment, and statutory law.[4] This content interception program is not in issue here.

The Motion To Dismiss

On July 28, 2006, AT&T filed a Motion to Dismiss ("MTD") on the ground that the Board lacks subject matter jurisdiction.[5] Fundamentally, AT&T's motion argues that the Board's jurisdiction over this matter has been preempted by federal law, "which wholly divests the states of any power to act with respect to matters of national security, national defense, and the gathering of foreign or military intelligence."[6]

---

3. This program was announced by President Bush and Attorney General Gonzalez in late 2004. *See* http://www.whitehouse.gov/news/releases/2005/12/print/20051219 1.html.

4. *American Civil Liberties Union v. National Security Agency*, ___ F.Supp. ____ slip op. at 2 (E.D. Mich., Aug. 17, 2006) (hereafter "*ACLU v. NSA*").

5. *See* V.R.C.P. 12(b)(1).

6. MTD at 2.

AT&T reports that this controversy may have arisen when, on May 11, 2006, the *USA Today* newspaper published a story suggesting that the NSA's intelligence-gathering activities may also have included some form of access to domestic call records databases.[7] AT&T contends that neither the government nor AT&T has confirmed or denied the accuracy of the reports or AT&T's participation.[8] Nevertheless, AT&T affirms that "any cooperation it affords the law enforcement or intelligence communities occurs strictly in accordance with law."[9]

AT&T reports that the United States Government ("USG") has repeatedly intervened to block lawsuits inquiring into the NSA Customer Records Program. According to AT&T, the USG "intends to assert the state secrets privilege in all of the pending actions brought and seek their dismissal."[10] For example, AT&T reports that the USG filed a motion to dismiss a federal lawsuit in California, arguing that "no aspect of [the] case can be litigated without disclosing state secrets."[11]

According to AT&T, the USG efforts have been successful, and two federal district courts have held that the NSA Customer Records Program is a state secret. In the California case ("*Hepting*"), the court barred discovery of any information relating to this claim, at least unless there are public disclosures of information relating to these allegations by the government.[12] AT&T recounts a similar result in the *Terkel* case in Illinois where the court dismissed the claims for similar reasons.

AT&T also recounts events in which the USG has acted to prevent state commissions from requiring disclosure relating to the NSA Customer Records Program. In New Jersey, the USG asserted that even disclosing whether materials exist relating to the NSA Customer Records Program "would violate various federal statutes and Executive Orders, including provisions that carry criminal sanctions."[13] The USG also sent a similar letter to AT&T, warning AT&T that

---

7. *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006, at A1.
8. MTD at 5.
9. MTD at 5.
10. MTD at 6.
11. MTD at 7. In that same case, the USG filed affidavits from the Director of National Intelligence ("DNI") and the Director of the National Security Agency. MTD at 8.
12. *Hepting v. AT & T Corp.*, ___ F.Supp. ___, 2006 WL 2038464 (N.D. Cal. June 20, 2006) ("*Hepting*").
13. MTD at 12 (internal quotations omitted).

""[r]esponding to the subpoenas - including by disclosing whether or to what extent any responsive materials exist - would violate federal laws and Executive Orders."[14] The USG has also filed suit against utility commissioners in Missouri.[15]

AT&T's central argument is that this docket violates the Supremacy Clause of the United States Constitution. First, AT&T argues that this docket directly conflicts with the federal Constitution itself, because the field of foreign intelligence gathering has been fully preempted by the constitution. Requiring AT&T to answer the Department's discovery would, according to AT&T:

> involve the state directly in functions that are exclusively federal: the defense of the nation against foreign attack. Under such circumstances, the state is without power to act, as theses matters are regulated and controlled exclusively by federal law. Moreover . . . the questions the Department seeks responses to regarding the NSA Program cannot be answered without confirming or denying facts that are not publicly disclosed and would risk harm to the United States' efforts to protect the nation against further terrorist attack.[16]

AT&T also contends that states are preempted by the so-called *Totten* rule from adjudicating any matters "concerning the espionage relationships of the United States."[17]

Aside from constitutional considerations, AT&T also argues that Congress has enacted a variety of statutes that fully preempt this field. AT&T contends that a:

> complex and comprehensive statutory scheme demonstrates that Congress has occupied the entire field with respect to the cooperation of telecommunications carriers with the federal government's intelligence-gathering and surveillance activities.[18]

AT&T also contends that the Department's discovery requests create conflicting duties: a disclosure duty to the state; and an opposing duty to the federal government. This, AT&T argues, is a classic example of conflict preemption.

AT&T argues that when "unique federal interests" such as foreign-intelligence gathering are involved, "[t]he conflict with federal policy need not be as sharp as that which must exist for

---

14. MTD at 12.
15. MTD at 13.
16. MTD at 14.
17. MTD at 22, 24.
18. MTD at 28.

ordinary pre-emption when Congress legislates in a field which the States have traditionally occupied."[19] This proceeding, AT&T argues, is "by its own account, related to the intelligence-gathering activities of the federal national security establishment that are designed to prevent further attacks on American soil as part of the nation's post-9/11 war effort," and is therefore entirely preempted.[20]

AT&T also asserts that this docket calls for disclosure of information which the USG has asserted to be covered by the state secrets privilege. State secrets is a constitutionally based privilege that "protects any information whose disclosure would result in impairment of the nation's defense capabilities or disclosure of intelligence-gathering methods or capabilities."[21] AT&T acknowledges that a state secrets claim "must be made formally through an affidavit by the head of the department which has control over the matter, after actual personal consideration by the officer," and AT&T asserts that the privilege cannot be waived by AT&T or any other private party.[22] This privilege, according to AT&T, covers every aspect of this docket, "even the mere existence or non-existence of any relationship between the federal government and AT&T Corp. in connection with this program."[23]

AT&T also contends that it is irrelevant that the United States has not formally invoked the state secrets privilege in this state administrative proceeding. According to AT&T, state secrets is a privilege that "is asserted in judicial proceedings where Article III judges review classified materials on an ex parte, in camera basis."[24] In state proceedings in New Jersey, AT&T explains that the USG did not assert the state secrets privilege, but AT&T nevertheless contends that knowing that the information has a security classification should mandate the same end.[25]

AT&T's motion also argues that two federal statutes independently preempt the Board's jurisdiction. The first is the prohibition on disclosing "classified information . . . concerning the

---

19. MTD at 21-22.
20. MTD at 23.
21. MTD at 19 (internal quotations omitted).
22. MTD at 19 (internal quotations and citation omitted).
23. MTD at 20.
24. MTD at 20.
25. MTD at 21.

communication intelligence activities of the United States."[26] AT&T notes that the USG raised this argument in the California and Michigan cases, and elsewhere, and it contends that the risk of criminal liability prevents it from participating here.

The second statute is the National Security Agency Act of 1959. This statute says that no law may require disclosure of any information with respect to the activities of the NSA.[27] AT&T argues that this Board should adopt the conclusion reached by the FCC, that "the National Security Agency Act of 1959 independently prohibits disclosure of information relating to NSA activities" and that this Board lacks "authority to compel the production of the information necessary to undertake an investigation."[28]

Participation by the United States Government

On July 31, 2006, the United States Department of Justice filed a letter on behalf of the USG ("DOJ letter"). The USG declined to intervene and asserted that its letter should not be deemed to be a "submission of the United States to the jurisdiction of Vermont."

Nevertheless, the DOJ letter takes a substantive position on the pending Motion to Dismiss. It argues generally that:

> the request for information and the application of state law they embody are inconsistent with and preempted under the Supremacy Clause, and that compliance with [the Department's Document Requests], and any similar discovery propounded by the [Board], would place [AT&T] in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without harming national security.[29]

The DOJ letter offers several legal grounds for preemption.

1. It argues that providing the requested information would interfere with the Nation's foreign-intelligence gathering, a field reserved exclusively to the Federal Government.[30]

2. It argues that providing the requested information would violate various statutes, including the National Security Agency Act and the Intelligence Reform and Terrorism

---

26. *See* 18 U.S.C. § 798.
27. *See* 50 U.S.C. § 402.
28. MTD at 18.
29. DOJ letter at 7.
30. DOJ letter at 3.

Prevention Act of 2004 as well as statutes and executive orders relating to classified information.[31]

3. It mentions, but does not clearly assert, the state secrets privilege. For example, the letter notes that court decisions on similar matters in another case "underscores that compliance with the requests for information would be improper."[32] The closest thing to a claim of privilege in the letter is an assertion that the state secrets privilege "covers the precise subject matter sought from [AT&T] by Vermont officials.[33]

The DOJ letter did not include any affidavits or sworn statement prepared for these dockets. It did include a photocopy of an affidavit submitted in a federal court proceeding by the Director of National Intelligence ("DNI") and asserting the state secrets privilege.[34]

Responses by the Department

On August 11, 2006, the Department filed a memorandum opposing the motion. The Department argues that the petition raises matters that do not implicate national security and that, if assertions in the petition are assumed to be true, the Department would be entitled to relief.

The Department's primary contention is that the scope of this proceeding exceeds what has been arguably preempted. The Department offers a distinction between the Board investigating the privacy of AT&T's Vermont customers and AT&T's company's compliance with state and federal privacy laws, on the one hand, and on the other, the details and propriety of national security programs or the workings of the NSA.[35] The Department contends that the claims here "fall squarely within the Board's authority."[36] The scope of this proceeding, argues the Department, extends beyond AT&T's interaction with the NSA, and extends to AT&T's interactions with all state and federal agencies.[37]

---

31. DOJ letter at 4-5.
32. DOJ letter at 5.
33. DOJ letter at 6.
34. DOJ letter, attachments from July 28 FAX at 16-17 (Negroponte statement at 4-5).
35. Response at 1-2.
36. Response at 3.
37. Response at 4. On this same basis, the Department argues that AT&T's reliance on *Terkel,* is misplaced. Response at 7.

In addition, the Department apparently makes a separate argument that federal preemption has not been demonstrated here. It contends, for example, that preemption of state law is possible only where a a federal agency acts within the scope of Congressionally delegated authority and makes clear its intent to preempt.[38]

The Department concludes by recommending that the Board "allow the investigation to proceed on all claims that are not directly related to the bulk disclosure of customer calling records to the NSA."[39] As to interactions with the NSA, the Department recommends denying the motion for now and reviewing after the evidence is in whether the government or AT&T have by that time confirmed the existence of the program.[40]

Also on August 11, the Department filed a letter responding to the DOJ letter. The letter notes that the USG has declined to intervene, and it argues that the Board should disregard the DOJ letter. The letter also argues that even where a state secrets privilege is asserted, the Board should carefully analyze whether the current circumstances warrant application of the privilege.

The letter also contends that the DOJ letter addressed only some of the issues in this docket. The Department specifically mentions AT&T's policies and practices regarding "maintaining and protecting private customer information, and whether [AT&T has] violated Vermont or federal disclosure laws, or [AT&T's] own policies."[41] For example, the Department asserts that AT&T could, consistent with its asserted privilege, answer a question about whether it has:

> disclosed any customer information that is deemed protected under state or federal law to any state or federal agency in the absence of a warrant, subpoena, court order or other applicable written authorization . . . .[42]

Reading the Department's August 11 letter and August 11 memorandum together, we conclude that the Department opposes the motion on two independent grounds: (1) the scope of

---

38. Response at 5, citing *Global NAPS, Inc. v. AT&T New England, Inc.*, ___ F.3d ___, 2006 WL 1828612, n.7 (2d Cir. 2006).

39. Response at 8.

40. Response at 8.

41. Letter at 2.

42. Letter at 2.

this docket is broader than the materials as to which there are claims of secrecy or privilege; and (2) the claims of secrecy and privilege have not been adequately established.

AT&T's Reply

On August 18, AT&T filed a reply. Initially, AT&T clarifies that its motion was filed on the ground that the Board lacks jurisdiction over this proceeding,[43] not that the petition fails to state a claim on which relief can be granted.[44] AT&T argues that the Department's response, which largely addressed the latter issue, was "beside the point."[45]

On substance, AT&T asserts that the Department's response "mostly seek to change the subject"[46] from federal preemption to state jurisdiction. AT&T accuses the Department of "semantic gamesmanship" in asserting that this docket is not about national security programs but about the privacy of Vermont customers.[47] The issue, AT&T maintains, is whether state regulation that otherwise would be allowable is nevertheless preempted because it interferes with foreign affairs.

AT&T contradicts the Department's assertion that the issues in this docket are broader than the NSA Customer Records Program. AT&T asserts that the Department's investigation "was inspired by, and relates directly to, the alleged participation of AT&T in communications intelligence activities of the NSA."[48] Moreover, AT&T asserts that to the extent this docket incidentally concerns disclosures to other federal agencies, inquiry into those disclosures, too, would be preempted, in part because the Board "has no power under the Constitution" to investigate such matters.[49]

As noted above, the Department had argued that AT&T could properly answer a question about whether it has disclosed customer information without specific authorization by warrant or

43. *See* V.R.C.P. 12(b)(1).
44. *See* V.R.C.P. 12(b)(6).
45. Reply at 2.
46. Reply at 4.
47. *Id.*
48. Reply at 3.
49. Reply at 4.

other means. AT&T contends that an answer to this question is not sufficient to determine whether any disclosures were unlawful since:

> [n]umerous provisions of federal law expressly envision that customer information might be intercepted or disclosed to government agencies without a warrant, subpoena, court order, or written authorization.[50]

Finally, AT&T disagrees with the Department's recommendation that this docket be left open because of the possibility of future public disclosures. Even if such disclosures were to occur, AT&T contends this Board would still lack jurisdiction to proceed with this docket.

II. Discussion

Standard for Motions to Dismiss

We consider AT&T's Motion to Dismiss as a Motion For Judgment on the Pleadings under Civil Rule 12(c).[51] To grant such a motion, this Board must take as true all well-pleaded factual allegations in the petition and all reasonable inferences drawn from those allegations. We must take as false all contravening assertions in AT&T's pleadings. We may grant the motion only if the petition contains no allegations that, if proven, would permit recovery.[52] To prevail, AT&T must show "beyond doubt that there exist no facts or circumstances that would entitle the [petitioners] to relief."[53]

State Law - Public Service Board Jurisdiction

As a matter of state law, the Board has jurisdiction over the claims asserted in the petitions. AT&T is a company offering telecommunications services on a common carrier basis in Vermont, and it therefore is a utility subject to the Board's jurisdiction.[54] That jurisdiction extends to the manner of operating and conducting that business, so as to ensure that the service

---

50. Reply at 5-6.

51. AT&T's motion is stated as under Rule 12(b)(1), which established the lack of jurisdiction over the subject matter as a basis for dismissal. Construing the motion under Rule 12(c) is not incompatible with the motion. Rule 12(b) requires certain defenses to be asserted in the first responsive pleading. By applying Rule 12(c), AT&T gains the opportunity to have us consider the motion as a motion for summary judgment, and thus to consider more than the pleadings.

52. *Knight v. Rower*, 170 Vt. 96 (1999).

53. *Union Mutual Fire Ins. Co. v. Joerg*, 2003 VT 27, 4, 824 A.2d 586, 588 (2003); Amy's *Enterprises v. Sorrell*, 174 Vt. 623, 623 (2002) (mem.).

54. 30 V.S.A. § 203(5).

is reasonable and expedient, and to "promote the safety, convenience and accommodation of the public.[55] The Board has broad supervisory jurisdiction over AT&T's operations in Vermont.[56] As to matters within its jurisdiction, the Board has the same authority as a court of record.[57] In addition, the Board has authority to impose civil penalties for an improper refusal to provide information to the Department or for violating a rule of the Board.[58]

The privacy of customer information has earned special mention in Vermont statutes. For example, when the Board considers a plan for alternative regulation of telecommunications companies, it must consider privacy issues.[59]

The Board's authority arises solely from statute, and it does not have jurisdiction over every claim that may involve a utility. For example, the Supreme Court has held that the Board has no jurisdiction over certain traditional torts merely because the defendant is a utility.[60] AT&T's motion, however, is not based upon any such limitation in state law.

Federal Law

AT&T's central contention is that federal law preempts matters that otherwise would be within the jurisdiction of the Board under state law.[61] We agree with AT&T that the supremacy clause of the United States Constitution allows federal law to preempt fully state and local laws.[62]

It is also true, however, that this Board ordinarily applies state law until it has been demonstrably preempted. Preemption can be established in a number of ways, including explicit

---

55. 30 V.S.A. § 209(a)(3).

56. *In re AT&T New England, Inc.*, 173 Vt. 327, 334-35 (2002).

57. 30 V.S.A. § 9.

58. 30 V.S.A. § 30.

59. *See* 30 V.S.A. §§ 226a(c) and 226(c)(8).

60. *E.g., Trybulski v. Bellows Fall Hydro-Elect. Corp.*, 112 Vt. 1 (1941) (Board did not have jurisdiction to assess damages for injuries to private landowners' properties allegedly caused by improper maintenance and operation of dam by hydro-electric company).

61. *See, e.g.* AT&T MTD at 3, note 1 ("state agencies lack jurisdiction with respect to matters relating to AT&T's alleged cooperation with federal national security or law enforcement authorities.")

62. U.S. Const. art. VI, cl. 2; *Crosby v. National Foreign Trade Council*, 530 U.S. 363, 372, 120 S.Ct. 2288, 147 L.Ed.2d 352 (2000)

or implicit statutory language, actual conflict, or occupation of the field.[63] Therefore, we undertake below to evaluate each of the theories advanced by AT&T as a basis for preemption.

State Secrets

The broadest challenge to the Board's jurisdiction is that these dockets involve state secrets. The state secrets privilege contains two distinct lines of cases.

Justiciability of Claims

The first line of cases is essentially a rule of "non-justiciability" that deprives courts of authority to hear suits against the Government based on certain espionage or intelligence-related subjects. The seminal decision in this line of cases is the 1875 decision in *Totten v. United States*.[64] The plaintiff in that case brought suit against the government seeking payment for espionage services he had provided during the Civil War. The Court's decision noted the unusual nature of a contract for espionage:

> The service stipulated by the contract was a secret service; the information sought was to be obtained clandestinely, and was to be communicated privately; the employment and the service were to be equally concealed. Both employer and agent must have understood that the lips of the other were to be for ever sealed respecting the relation of either to the matter. This condition of the engagement was implied from the nature of the employment, and is implied in all secret employments of the government in time of war, or upon matters affecting our foreign relations, where a disclosure of the service might compromise or embarrass our government in its public duties, or endanger the person or injure the character of the agent.[65]

Given the unusually secret nature of these contracts, the Court held that no action was possible for their enforcement. Indeed, "[t]he publicity produced by an action would itself be a breach of a contract of that kind, and thus defeat a recovery."[66]

The Supreme Court recently reaffirmed this principle in *Tenet v. Doe*.[67] In *Tenet*, the plaintiffs, who were former Cold War spies, brought estoppel and due process claims against the

---

63. *See, e.g., In re AT&T New England, Inc.*, 173 Vt. 327, 336 (2002).
64. 92 U.S. 105 (1875).
65. *Totten*, 92 U.S. at 106.
66. *Totten*, 92 U.S. at 107.
67. *Tenet v. Doe*, 544 U.S. 1, (2005).

United States and the Director of the Central Intelligence Agency for its alleged failure to provide them with the assistance it had allegedly promised in return for their espionage services.[68] Relying heavily on *Totten*, the Court held that the plaintiffs' claims were barred. For a unanimous Court, Chief Justice Rehnquist wrote:

> We adhere to *Totten*. The state secrets privilege and the more frequent use of in camera judicial proceedings simply cannot provide the absolute protection we found necessary in enunciating the Totten rule. The possibility that a suit may proceed and an espionage relationship may be revealed, if the state secrets privilege is found not to apply, is unacceptable. Even a small chance that some court will order disclosure of a source's identity could well impair intelligence gathering and cause sources to 'close up like a clam.'[69]

The *Totten/Tenet* principle, where applicable, provides an absolute bar to any kind of judicial review, and therefore would also bar any quasi-judicial proceeding by a state agency.[70]

The *Totten/Tenet* rule is inapplicable here. It applies to actions where there is a secret espionage relationship between the Plaintiff and the Government.[71] Petitioners here do not claim to be spies or to have any form of secret espionage relationship with the government. Therefore the absolute bar rule does not apply to these dockets.

Evidentiary Privilege

The second branch of the State secrets doctrine deals with the exclusion of evidence, and the consequences of that exclusion.

The effect of the state secrets privilege on plaintiffs is like other evidentiary privileges. Where a privilege blocks admission of some evidence, a plaintiff nevertheless may use other evidence to prove his or her case. However, if the plaintiff fails to carry its burden of proof, the court may dismiss the case or grant summary judgment against the plaintiff, as in any other proceeding.[72]

---

68. *Tenet* at 3.

69. *Tenet* at 11 (citations omitted).

70. *Tenet* at 8.

71. *Tenet* at 7-8; *ACLU v. NSA* at 10-11; cf. *Terkel*at 15-16 (declining to extend *Totten* principle to disclosure of telephone records to the government because such disclosures are not inherently harmful to national security and would reveal violations of plaintiffs' statutory rights).

72. *United States v. Reynolds*, 345 U.S. 1, 11 (1953); *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C.Cir. 1983).

For defendants, the state secrets privilege produces the opposite of the normal result. Normally a defendant who needs privileged evidence admitted into evidence is harmed by the privilege. With the state secrets privilege, however, the defendant gains an advantage. Where a defendant needs evidence comprising a state secret in order to create a valid defense, summary judgment must be granted to the defendant.[73]

For two independent reasons, we deny the Motion to Dismiss on grounds of the state secrets privilege.

1. AT&T has not properly invoked the privilege

The United States Supreme Court has explained that the state secrets "privilege belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party. Moreover, there must be a "formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer."[74]

Here, the government has declined to become a party, despite our earlier invitation to do so.[75] AT&T is a party, but under federal law it does not have standing to raise the privilege. Moreover, no party has submitted any sworn statement prepared for these dockets. Instead, both AT&T and the DOJ letter included photocopies of affidavits filed in other proceedings by the Director of National Intelligence.[76]

A motion to dismiss may be treated as a motion for summary judgment if it involves matters outside the pleadings.[77] Since the DOJ letter is not a pleading, we could grant summary judgment for AT&T if the record shows that there are no material facts that are genuinely in

---

73. *Kasza*, 133 F.3d at 1166; *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1141 (5th Cir. 1992). Normally a defendant relying on privileged evidence would be deprived of that evidence, and might thereby lose a valid defense. However, by requiring dismissal in such cases, the state secrets privilege uniquely operates to benefit defendants in all cases, regardless of which party needs the secret evidence.

74. *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *Hepting* at 16.

75. As noted above, the Department of Justice declined to intervene and asserted that its letter should not be deemed to be a "submission of the United States to the jurisdiction of Vermont." We are puzzled by this statement because we are not aware that when the United States intervenes in a state administrative proceeding the form gains "jurisdiction" over the federal government.

76. *E.g.*, DOJ letter, attachments from July 28 FAX at 16-17 (Negroponte statement at 4-5).

77. V.R.C.P. 12(c).

dispute. Partial summary judgment can also be granted when only some issues are in dispute.[78] Summary judgment can be granted without affidavits,[79] but affidavits can be used to show that no material issue of fact exists. Where affidavits are submitted, they must be based upon personal knowledge.[80]

We noted above that federal law requires the government to claim the state secrets privilege. This is not an empty formality. Because the privilege, once accepted, creates an absolute bar to the consideration of evidence, the courts do not lightly accept a claim of privilege. In each case, the government's showing of necessity for the privilege determines "how far the court probes in satisfying itself that the occasion for invoking the privilege is appropriate."[81] The courts have made it clear that "control over the evidence in a case cannot be abdicated to the caprice of executive officers.[82] The privilege may not be used to shield any material not strictly necessary to prevent injury to national security; and, whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.[83]

Federal courts have frequently conducted *in camera* proceedings to test the assertion of the privilege.[84] In the recent *Terkel* case, the government has voluntarily filed both public and secret *in camera* affidavits for the courts' consideration.[85] We recognize that *in camera* proceedings before this Board may present difficulties that do not arise in federal courts. However, we understand the relevant federal law to require not only that the privilege be claimed by the responsible official but that the trier of fact at least minimally test whether "the occasion for invoking the privilege is appropriate."[86] We are not convinced that those difficulties cannot be overcome.[87]

---

78. V.R.C.P. 12(d). Summary judgment cannot be granted, however, without offering the parties a reasonable opportunity to present material pertinent to the motion. V.R.C.P. 12(c).

79. V.R.C.P. 56(b).

80. V.R.C.P. 56(e); *Department of Social Welfare v. Berlin Development Assoc.*, 138 Vt. 160 (1980).

81. *U.S. v. Reynolds*, 345 U.S. at 11.

82. *U.S. v. Reynolds*, 345 U.S. at 11.

83. *Ellsberg v. Mitchell*, 709 F.2d 51, 56 (D.C. Cir. 1983).

84. *E.g., Hepting* at 4; *Terkel* at 5, 21.

85. *Terkel* at 5. The DOJ letter here attached a photocopy of the affidavit from *Terkel.*

86. *U.S. v. Reynolds* at 11.

87. *See* discussion below of CIPA rules for sharing of classified information in "graymail" cases.

The privacy issued raised in these dockets are of great interest to Vermont ratepayers, and we are not willing to dismiss this proceeding without, at minimum, affidavits sufficient to justify that action. Therefore we hold that the government's claim of privilege must be accompanied by at least some admissible evidence, ordinarily by affidavit, from a responsible official who asserts after personal consideration that the subject matter is a state secret.[88] No such affidavit has been submitted in this proceeding. Therefore the state secrets privilege has not been properly claimed here.

2. The state secrets privilege, if it did apply, would not bar all pending claims.

If the Department cannot prove that AT&T has participated in the NSA Customer Records Program, it may still be entitled to some relief here. For example, the Department may request the Board to order AT&T to modify its existing customer privacy notices to describe the policies that AT&T would apply in the *hypothetical* event that AT&T is asked in the future to disclose confidential customer information pursuant to a secret government program. Even if this Board cannot consider what *has* happened, we are not preempted from requiring AT&T to provide notice to customers describing how AT&T would apply the known structures of federal law to government requests for otherwise private information.[89]

As noted above, AT&T has asserted that "any cooperation it affords the law enforcement or intelligence communities occurs strictly in accordance with law."[90] AT&T also asserts, however, that "[n]umerous provisions of federal law expressly envision that customer information might be intercepted or disclosed to government agencies without a warrant, subpoena, court order, or written authorization."[91] The Department may legitimately seek more information regarding AT&T's beliefs about the circumstances under which the law allows such interception and disclosure. In particular, the Department may want to know more about the circumstances under which AT&T believes that it may disclose customer information without

---

88. *See, e.g., Hepting*at 16 (state secret privilege requires a formal claim by agency head after personal consideration).

89. This point is underscored by the breadth of the claims in AT&T's filings and in the DOJ letter. Those documents demonstrate that, regardless of what AT&T has done in the past, if it were to agree in the future to provide the NSA with customer record information, AT&T would consider itself barred from disclosing that fact.

90. MTD at 5.

91. Reply at 5-6.

warrants, written findings or other documents. These facts also might appropriately influence the content of customer notices and the company's written privacy policies.

Field Preemption

AT&T and the USG argues that providing the requested information would interfere with the Nation's foreign-intelligence gathering, a field reserved exclusively to the Federal Government.[92] They argue: (1) the field of foreign-intelligence gathering has been fully preempted; and (2) this prevents any and all state inquiry into communications between AT&T and the NSA that USG describes as part of the USG's foreign-intelligence gathering efforts. While the first proposition above may be true, the second requires proof.

We reject the field preemption argument for procedural reasons. As we noted above, the USG has not appeared in this proceeding and has not offered any sworn evidence supporting its position. Instead, it has provided photocopies of affidavits it submitted in other proceedings. It is not enough, as the USG asserts, that a high government official recently told a federal court in another state that this subject involves national security.

AT&T also argues that federal legislation preempts the field, which it defines as "the cooperation of telecommunications carriers with the federal government's intelligence-gathering and surveillance activities."[93] AT&T cites the Communications Assistance to Law Enforcement Act ("CALEA"),[94] the Wiretap Act,[95] the Stored Communications Act,[96] and the Foreign Intelligence Surveillance Act (FISA).[97] AT&T concludes that this complex federal scheme leaves no room for state regulation of an exclusively federal function.

We reject this statutory argument. It is true that a variety of federal statutes exist that regulate the relationship between telecommunications carriers and federal police agencies. While many aspects of the relationship between telecommunications carriers and police have indeed been so defined, AT&T fails to show that this fully preempts the field. For example, states differ

92. DOJ letter at 3.
93. MTD at 28.
94. *See* 47 U.S.C. § 1001 *et seq.*
95. *See* 18 U.S.C. § 2511 *et seq.*
96. *See* 18 U.S.C. § 2701 *et seq.*
97. *See* 50 U.S.C. § 1804(a)(4); 50 U.S.C. § 1805(c)(2).

among themselves regarding the requirements for wiretap warrants. If the relationship between police agencies and telecommunications carriers can vary by state, the field has not been preempted by comprehensive Congressional enactments.

Statutory Arguments

The NSA Statute

AT&T and the DOJ letter assert that Section 6(a) of the National Security Agency Act of 1959 ("NSA Statute") requires dismissal. This statute provides:

> Sec. 6. (a) . . . [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 the persons employed by such agency.[98]

On its face, this statute is extraordinarily broad. By its terms, it trumps *any* "other law," state or federal. One federal court, commenting on the breadth of this statute observed that if this statute were:

> taken to its logical conclusion, it would allow the federal government to conceal information regarding blatantly illegal or unconstitutional activities simply by assigning these activities to the NSA or claiming they implicated information about the NSA's functions.[99]

Courts have nevertheless applied the statute as written. For example, the statute gives the NSA the absolute right to resist a Freedom of Information request seeking disclosure of information from the NSA's own files regarding its own operations.[100]

AT&T's interpretation would further expand the reach of the statute. AT&T argues: (1) it may have provided information to the NSA; and (2) requiring it to now explain what it did would improperly disclose the activities of the NSA.

This interpretation not only protects NSA employees, officers and files from forced disclosures, but it would also apply the statute to people with whom the NSA has had contact and from whom it has requested information. The argument seems to be a form of "Midas Touch" for the NSA: anything it touches becomes secret. Once the USG has asserted that the activities

---

98. Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note.

99. *Terkel*at 11.

100. *Id.*; *Hayden v. National Security Agency*, 608 F.2d 1381 (D.C. Cir. 1979).

of *any* private person also relate to NSA activities, the USG's argument seems to require that the activity as a whole becomes privileged and all state inquiry about that activity must cease, regardless of the consequences to petitioners, respondents, utilities and customers. This goes far beyond the scope of a statute nominally aimed at keeping confidential the names, salaries and activities of NSA employees. Moreover, courts have made clear that a simple assertion that Section 6(a) applies is inadequate. For example, in *Founding Church of Scientology v. NSA*, the Court of Appeals for the District of Columbia rejected the District Court's reliance upon an affidavit from the NSA invoking Section 6 when that affidavit made simple conclusory assertions which were not substantiated.[101] Here, AT&T has simply made broad assertions, unsupported by an affidavit by the NSA. Therefore, we conclude that AT&T has not presented a sufficiently detailed basis for us to find that Section 6(a) bars disclosure of all information that may be relevant to this proceeding.

Even though the courts have applied Section 6(a) broadly, for an independent reason it does not support dismissal at this time. In the *Hepting* case in Northern California, Judge Walker denied dismissal of similar claims, even though he blocked discovery on those same claims. He noted the possibility that the government or the defendant telecommunications carrier might make public disclosures that would support the claims made in that case. Instead of dismissing the case, the judge offered to make step-by-step determinations during discovery as to whether the various privileges would prevent plaintiffs from discovering evidence.[102]

We have decided to follow the same course. AT&T or other utilities who participated in the NSA Customer Records Program may make further disclosures that are sufficiently reliable to alter the outcome. Although some of the petitioner's discovery requests may be blocked by one or another privilege, some information about AT&T's activities may nevertheless emerge. Later, AT&T might be entitled to summary judgment if the state secrets privilege blocks certain items of evidence that are essential to plaintiffs' prima facie case or to AT&T's defense. Alternatively, time may provide petitioners more non-classified and admissible materials, and it is at least conceivable that some of petitioner's claims could survive summary judgment. As

---

101. 610 F.2d 824, 831–833 (1978).

102. *Hepting* at 21.

discovery proceeds, we will be willing to determine step-by-step whether the privilege prevents petitioner from discovering particular evidence. The mere existence of the NSA statute, however, does not justify dismissing this docket now.

Foreign Intelligence Surveillance Act

The DOJ letter asserts that AT&T may not provide information by a provision of the Foreign Intelligence Surveillance Act ("FISA"). These statutes relate to the terms of judicial FISA orders authorizing electronic surveillance. They allow a court issuing a surveillance warrant to direct a common carrier to cooperate in executing that warrant and also to direct that the carrier protect the secrecy of the surveillance while minimally interfering with the target's normal services.[103] The statutes also allow the court to require the carrier to keep records of the surveillance.[104]

These statutes are irrelevant. Nothing in the record suggests that AT&T ever received a FISA warrant regarding the NSA Customer Records Program.

As noted above, the federal government operates a program of warrantless interception of certain communications involving persons suspected of having contacts with al Qaeda has recently been reviewed in the courts. One court has held that this program violates FISA because the program "has undisputedly been implemented without regard to FISA."[105] If the United States government operates its content interception program without recourse to FISA, we see little reason to infer that it would use those procedures to obtain disclosure of telecommunications records.

Classified Information

AT&T also moves to dismiss on the grounds that if it has participated in the NSA Customer Records Program, that program, and AT&T's participation, would be classified information. As a result, if AT&T were required to provide such information it would be

---

103. 50 U.S.C. § 1805(c)(2)(B).
104. 50 U.S.C. § 1805(c)(2)(C).
105. *ACLU v. NSA* at 2.

subject to prosecution for a felony.[106] Therefore, AT&T argues that the federal classification imposes conflicting state and federal duties, in which the federal duty must be supreme.

The DOJ letter asserts that various Executive Orders require that classified information cannot be disclosed unless the head of the agency imposing the classification has authorized disclosure, the recipient has signed a nondisclosure agreement, and the person has a need-to-know.[107] According to the DOJ, Vermont state officials do not qualify.

Initially, we note that the DOJ letter suggests that a very broad category of information is classified. The DOJ letter asserts the claim for any and all matters relating to the "foreign-intelligence activities of the United States."[108] Given the context, however, this also includes domestic data collection activities. In this sense, the USG defines "foreign-intelligence" by the purpose of the activity, not the location at which the information is collected.

We also note that this dispute does not involve a party seeking disclosure of information held in government files or a party seeking to compel the testimony of a government official or employee. Instead, the alleged classified activity involves the activities of civilian employees of a telecommunications company regulated in Vermont. The petitioners assert that AT&T may have transferred data to the government or even given the government access to customer information and calling patterns contained in the utility's files. Therefore what is putatively classified here is the knowledge of AT&T's officials and employees, and that knowledge may consist of nothing more than network design information or software access information.

"Graymail" is a practice by criminal defendants in which the defendant seeks to avoid prosecution by threatening to disclose classified materials in open court.[109] Congress enacted a statute to deal with this problem, the Classified Information Procedures Act (CIPA).[110] Under CIPA, when it appears that classified information may be disclosed in a criminal case, any party may move for a pretrial conference to consider rules for discovery and disclosure of that

---

106. 18 U.S.C. § 798(a)(1) prohibits making available to an unauthorized person any "classified information" relating to the "communications intelligence activities of the United States."

107. DOJ letter filed 7/31/06 at 4-5.

108. DOJ letter at 5.

109. In these cases the USG is often already a party.

110. 18 U.S.C.A. App. §§ 1-16.

information.[111] A defendant may not disclose classified information at trial without giving advance notice to the Attorney General,[112] who can then request a hearing to protect the information.[113] The court must conduct a hearing if one is requested, and the hearing may be held *in camera.*[114] Where a defendant seeks and ultimately receives classified information, the court can enter an order preventing further disclosure.[115] When the Attorney General submits an affidavit certifying that information is classified, the court may authorize the government to submit redacted documents, to submit summaries of documents, or to admit relevant facts.[116]

Under CIPA, court personnel have access to classified information. To facilitate this process, the Chief Justice of the United States has determined that no security clearances are required for judges, and security clearances have been sought for other court personnel.[117] The government can even compel defense counsel to undergo a DOJ initiated security clearance procedure,[118] and classified information can be provided to the defendant's counsel.[119]

Like CIPA, these dockets present a conflict between a party's rights (and need for evidence to exert those rights) and the government's need to keep the information from disclosure because of its potential harm to national security interests.[120] We find it instructive that CIPA allows a criminal court wide latitude to balance these interests and to use tools such as security clearances, closed hearings, redaction, summaries and protective orders. We also find it instructive that the government in CIPA cases has offered (and even mandated) security clearances for criminal defense counsel. It is disappointing that the USG has not offered to use any such limiting techniques in this proceeding. Nevertheless, CIPA does not apply here. While we might wish the law were otherwise, we have no legal authority to insist upon CIPA-like

---

111. *See* 18 U.S.C.A. App. § 2.
112. *See* 18 U.S.C.A. App. § 5(a).
113. *See* 18 U.S.C.A. App. § 6(a).
114. *See* 18 U.S.C.A. App. § 6(a).
115. *See* 18 U.S.C.A. App. § 3.
116. *See* 18 U.S.C.A. App. § 6(c)(2).
117. *U.S. v. Jolliff*, 548 F.Supp. 229, 231 (D. Md. 1981).
118. *U.S. v. Bin Laden*, 58 F.Supp.2d 113 (S.D.N.Y. 1999).
119. *Jolliff, Bin Laden*, above.
120. CIPA also involves other constitutional rights such as the right to assistance of counsel and the right to confront adverse witnesses in criminal cases.

procedures. Yet, it is unfortunate that thousands of Vermont's citizens' right to privacy does not receive similar procedural protection.

The issue here, therefore, is whether we should deny relief to the petitioner in this proceeding because the petition seeks information that may be classified. In deciding this question, we return again to the key fact that there is no sworn evidence or affidavits on any of these matters. We conclude that there is no evidentiary basis to find that federal classification systems will prevent us from reaching a decision in this matter. Unlike CIPA cases in which the government must present an affidavit opposing release of classified information, here we have only a letter and a photocopy of an affidavit submitted elsewhere. This does not provide an adequate basis to dismiss the petition.

In addition, as we did above, we rely on the possibility of future disclosures. As the *Hepting* court found, reliable public disclosures between now and the time that this case is decided may allow petitioner to establish a right to relief independent of classified information.

Intelligence Reform and Terrorism Prevention Act of 2004

The USG asserts that requiring AT&T to reply to discovery in this docket would violate the Intelligence Reform and Terrorism Prevention Act of 2004.[121] This statute gives the Director of National Intelligence ("DNI") the authority to "protect intelligence sources and methods from unauthorized disclosure."[122]

This statute is clear on its face. It imposes a duty on the DNI, not on this Board. One might argue that this statute obligates the DNI to intervene in these proceedings to protect intelligence sources. It might even be arguable that this statute gives the DNI a defense to an action seeking disclosure of information he holds. The statute clearly does not, however, create a duty for this Board to dismiss dockets brought by customers and the Department against a utility.[123] It certainly does not requires us to do so without receiving evidence that draws a connection between the evidence sought and the sworn evidence that this intrudes upon the government's intelligence sources and methods.

---

121. DOJ letter at 4.

122. Pub. L. No. 108-458, 118 State. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1).

123. *Terkel*, slip op. at 12.

III. CONCLUSION

We deny AT&T's Motion to Dismiss because we have jurisdiction under state law to proceed in this matter, and it has not been shown that federal law preempts that jurisdiction. Moreover, we conclude that there is the possibility that facts will be adduced to sustain petitioners' claims. We recognize that the Department may now seek discovery of a sort recently prohibited by two federal district courts. However, we believe that the better approach is to limit discovery on a more particularized basis.

SO ORDERED.

Dated at Montpelier, Vermont, this 18th day of September, 2006.

s/ James Volz)
)
) PUBLIC SERVICE
)
s/ David C. Coen) BOARD
)
) OF VERMONT
s/ John D. Burke)

OFFICE OF THE CLERK

FILED: September 18, 2006

ATTEST: s/ Susan M. Hudson
Clerk of the Board

NOTICE TO READERS: This decision is subject to revision of technical errors. Readers are requested to notify the Clerk of the Board (by e-mail, telephone, or in writing) of any apparent errors, in order that any necessary corrections may be made. (E-mail address: psb.clerk@state.vt.us)

*2004 Ore. PUC LEXIS 10, **

In the Matter of a Proposed Rulemaking, related to Open Network Architecture, to Repeal rules in Division 035 of Chapter 860 of the Oregon Administrative Rules and to Adopt OAR **860-032-0510,** related to Customer Proprietary Network Information, and OAR 860-032-0520, related to Customer Service Records

ORDER NO. 04-012; AR 469

Oregon Public Utility Commission

2004 Ore. PUC LEXIS 10

January 8, 2004, Entered

CORE TERMS: customer, carrier, telecommunication, enhanced, collocation, network, provider, requesting, virtual, staff, migration, space, tariff, implemented, disclose, unbundled, proprietary, rulemaking, format, competitive, workshops, authorization, aggregate, cooperative, subscriber, software, billing, telephone number, proposed rule, interexchange

DISPOSITION: [*1] NEW RULES ADOPTED, DIVISION 035 RULES REPEALED

PANEL: Lee Beyer, Chairman; John Savage, Commissioner; Ray Baum, Commissioner

OPINION: ORDER

This rulemaking covers several different matters. We repeal rules in Division 035 in part because several of the rules were invalidated by an Oregon Supreme Court decision, and in part because federal law has made that division of rules obsolete. We adopt the Customer Proprietary Network Information Rule, proposed OAR **860-032-0510,** which is a modified version of a rule already in effect, changed only to mirror federal law. Finally, we adopt the rule dealing with migration between competitive local exchange carriers, OAR 860-032-0520, which stems from an earlier investigation, docket UM 1068, and any comments made in that proceeding are considered here also.

PROCEDURE

At the September 11, 2003, public meeting, the Commission opened this rulemaking proceeding. Notice of the rulemaking and a statement of fiscal impact were filed with the Oregon Secretary of State on September 15, 2003. Notice of the rulemaking was published in the Oregon Bulletin on October 1, 2003. A comment period was held; originally it was set to expire October 21, 2003, and it was extended **[*2]** until November 14, 2003. In addition, a comment hearing was held on October 28, 2003. Verizon Northwest Inc. (Verizon), Qwest Corporation (Qwest), AT&T Telecommunications of the Pacific Northwest, Inc. (AT&T), and Commission Staff (Staff) submitted comments, which were considered and are discussed below.

Draft rules OAR **860-032-0510** and 860-032-0520 were originally developed during extensive workshops in UM 1068, which was an earlier investigation into rules that would govern the migration of customers between competitive local exchange carriers. On October 16, 2002, Allegiance Telecom of Oregon, Inc. (Allegiance), petitioned the Commission to open a docket to investigate what rules should govern the migration of customers between competitive local exchange carriers, modeled on rules considered by the New York Public Service Commission. Petitions to intervene were filed by Qwest, Verizon, AT&T, GVNW Consulting, Inc., Electric Lightwave, Inc., Worldcom, Inc., Time Warner Telecom of Oregon

LLC, Oregon Telecommunications Association, PriorityOne Telecommunications, Inc., Oregon Telecom, Inc., Integra Telecom of Oregon, Inc., and Covad Communications, Inc. These parties and Staff met **[*3]** for workshops on December 18, 2002 and May 2, 2003, and for a teleconference on July 9, 2003. Written comments were received from GVNW Consulting, Oregon Telecommunications Association, and Covad Communications. The Commission closed docket UM 1068 without order during the same public meeting in which it opened this docket.

In this docket, we repeal all of the rules in Division 035 of the administrative rules and adopt two new rules, and our discussion is organized accordingly.

DIVISION 035

Division 035 of the Commission's rules provides for Open Network Architecture for telecommunications providers. The rules in this division were first adopted in 1993 to permit enhanced service providers (ESP) to use parts of local exchange carrier (LEC) networks to provide services to customers.

Some of the rules were invalidated by the Oregon Supreme Court in *GTE Northwest, Inc. v. Public Utility Commission,* 321 Or 458, 900 P2d 495 (1995). To the extent that the rules required that LECs open their facilities to use by ESPs, the court found that the rules were an unconstitutional taking of property under the state and federal constitutions. The **[*4]** court held that the Commission "does not have express statutory authority to promulgate rules that would effect a taking of an LEC's facilities," 321 Or at 468, and "the challenged collocation rules effect a taking," 321 Or at 477. As a consequence, the court invalidated OAR 860-035-0020(8), 860-035-0070(5), and 860-035-0110.

Since then, the Telecommunications Act of 1996 was enacted. The Act requires incumbent local exchange carriers (ILECs) to provide unbundled network elements of their networks to competitive local exchange carriers (CLECs) and to allow CLECs to physically collocate equipment in the ILECs central offices. ESPs now buy the services they need through the utilities' tariffs or from the CLECs, so the rules in Division 035 are no longer necessary. No participant in the rulemaking process expressed opposition to the repeal of the rules in Division 035.

Because they have been invalidated in part and related issues have been dealt with on the federal level, the rules in Division 035 are repealed.

OAR 860-032-0510

The proposed rule regarding Customer Proprietary Network Information **[*5]** (CPNI) is a modified version of OAR 860-035-0090, first adopted in 1993 and amended in 1997. This rule is designed to protect customer privacy regarding telecommunications services.

Currently, the rule states that a carrier may disclose CPNI to a third party only after the customer has authorized the disclosure. FCC rules, by contrast, contain an elaborate "opt-in/opt-out" process that allows carriers to disclose CPNI to third parties unless the customer affirmatively opts out. Proposed OAR **860-032-0510** clarifies the current rule so that it more closely mirrors federal law and new FCC rules. It also eliminates the requirement that a carrier obtain customer consent before releasing the customer's CPNI. By aligning the state rules with federal rules, we will make it easier for carriers to know what procedures they must follow. Staff also explained that it would be easier to deal with violations of the rule if the federal requirements are added to state rules. No participant in the rulemaking process expressed opposition to adoption of proposed OAR **860-032-0510.** We adopt the changes and renumber it to OAR **860-032-0510** because the rules in Division 035 are being repealed in this order.

[*6]
OAR 860-032-0520

This new rule governs how telecommunications carriers share information about a customer who migrates from one CLEC to another. The shared information, called a Customer Service Record (CSR), includes billing information, a working telephone number, current interexchange carrier, custom calling features in use, and circuit ID. According to the Staff report that recommended opening this docket,

> as requested by the participating telecommunication providers, the scope of the proposed rule is limited to exchange of CSR information. The exchange of CSR information precedes actual customer migration from one carrier to another. The proposed rule does not deal with actual customer migration. Other steps, which the industry did not want considered in this rulemaking, include local service requests (LSRs), whereby the new carrier requests the old carrier to migrate or transfer the customer, and the actual steps of transferring the customer to the new carrier.

Staff Report, Public Meeting September 11, 2003, Item No. CA8 and CA9, at 2-3. Proposed OAR 860-032-0520 is set forth in Appendix A. The purpose of the rule is to provide procedures for a requesting local **[*7]** service provider (LSP) to acquire information from the current LSP so that customer migration is seamless and timely. The rule applies to carriers that do not have an approved interconnection agreement with the requesting LSP that addresses the requirements covered by this rule; the rule does not apply to carriers with such an approved interconnection agreement or to cooperatives. This rule sparked numerous comments from the telephone companies during both UM 1068 and the rulemaking process, which we discuss in turn.

UM 1068 comments

Several written comments were submitted previously in UM 1068. GVNW Consulting and the Oregon Telecommunications Association supported the principles in the New York Public Service Commission guidelines regarding CLEC to CLEC migration, which were provided as a supplement to Allegiance's petition to open docket UM 1068. Covad Communications also supported New York's guidelines but recommended that Oregon go further and address customer migration from ILEC to CLEC. Those comments, as well as others made at the workshops, were integrated into the proposed rule used to initiate this docket. Official notice has been taken of those comments, and we also **[*8]** consider them in adopting this rule.

Qwest

Qwest articulated two major concerns with the proposed rule. First, Qwest preferred that CSRs be transmitted using the responding carrier's format, rather than the requesting carrier's format as prescribed in proposed subsection (7)(a)(C). In addition, subsection (7)(b)(C) states that a CSR may include a tracking number; Qwest suggested that a tracking number only be used if required by the responding carrier's format.

Second, Qwest proposed several changes to eliminate the requirement that the unbundled network element loop (UNE-L) be reused if possible. Qwest characterized the reuse of UNE-L facilities as a technical matter beyond the scope of this rule. Accordingly, it recommended deleting the parts of the rule related to sharing circuit ID information or reusing UNE-L facilities in subsections (7)(a)(F), (9), and (11). Qwest also recommended editing subsection (10) so that the responding LSP does not have to disclose the customer's PIC freeze status

and local freeze status in the CSR, reasoning that the new LSP can change the freeze status and that nondisclosure will not prevent migration of customers.

At the hearing, Staff opposed **[*9]** Qwest's written comments. Staff noted that Qwest had participated in the workshops in UM 1068 and that the participants in the workshops compromised to produce the proposed rule. Qwest's proposed changes at this stage of the proceedings are too late, in Staff's view.

We decline to adopt Qwest's proposed changes. First, the CSRs should be transmitted using the requesting LSP's format in order to facilitate movement between LSPs. If this format poses a problem in the future, the parties may raise the issue later. Second, contrary to Qwest's suggestion, facilities should be reused if possible to minimize costs to new carriers and to ease migration and promote competition. Consequently, we will retain the requirement that facilities be reused if possible. For these reasons, we decline to adopt Qwest's suggested changes to the rule.

Verizon

In its written comments, Verizon supported the proposed rule with one minor clarification: changing the phrase in subsection (1) from "so a customer can *change* local exchange service" to "so a customer can *migrate* local exchange service." Verizon Comments, filed October 14, 2003, at 1. We adopt the clarification.

The company also noted that **[*10]** it looks forward to additional workshops in a rulemaking docket for customer migration. Staff responded at the hearing that it did not agree that additional workshops would be necessary. This rule only deals with the first stages of CLEC-to-CLEC migration; if further rulemaking dockets are opened to deal with other parts of migration, then additional workshops may be necessary.

AT&T

At the hearing and in subsequent written comments, AT&T raised two concerns. First, AT&T proposed amending the rule so that a new LSP can request a CSR from the underlying network service provider (NSP) as well as the former LSP. It reasoned that the NSP will have to examine the information anyway, and the NSP is more likely to have accurate information for the CSR than the LSP. In addition, AT&T notes that it has adopted "electronic interfaces to receive CSRs from the ILECs, which are based on unique ILEC specific business rules." AT&T Comments, filed October 31, 2003, at 3. AT&T recommended that CLECs also use the same format.

Verizon opposed AT&T's recommendation that the NSP should also be responsible for providing CSRs to a requesting LSP. Verizon stated that the current LSP should bear the burden **[*11]** of ensuring that the information in the CSR is accurate. Further, Verizon resisted the idea of having to adopt a particular format for the CSR, as recommended by AT&T. Staff also opposed requiring an NSP to be responsible for CSRs. In its opening comments, Staff stated that it "believes that it is better policy" for the old LSP alone to provide the information and that requiring both to provide the CSR will "invite[] confusion or duplication." Staff Comments, filed October 21, 2003, at 4.

Second, AT&T recommended that the timing requirement be made more flexible. As written, the rule requires a two-day, and later a one-day, turnaround unless the responding LSP give notice and "a legitimate reason." AT&T suggested that the rule allow for an 80% compliance rate with the one- to two-day deadline.

Staff noted that the timing requirements were "addressed in considerable detail" by the participants in the UM 1068 workshops, including AT&T. At that time, the participants

rejected a compliance benchmark,

> because of the increased record keeping requirements. It also was rejected because such a requirement would necessarily involve PUC Staff in disputes about whether the 80% benchmark had **[*12]** been achieved. Staff believed and believes any perceived benefit of such a benchmark is greatly outweighed by the burden on Staff's already strained and limited resources.

Staff Comments, filed November 4, 2003, at 2.

Both proposals raised by AT&T were thoroughly discussed and rejected in UM 1068 by other telecommunications carriers and Staff, and we also decline to adopt those suggestions. Requiring both the NSP and the current LSP to provide a CSR on request would result in a duplication of work and confusion between the NSP and LSP as to which entity is responsible for providing the CSR. In addition, an 80% benchmark for meeting the time requirement would put additional responsibilities on Staff for investigating and monitoring compliance. As a result, we decline to adopt either of AT&T's suggestions.

ORDER

IT IS ORDERED that:

1. The rules in Division 035 are repealed.

2. Proposed OARs **860-032-0510** and 860-032-0520, attached as Appendix A, are adopted.

3. The new rules and the repeal of the rules in Division 035 shall be effective upon filing with the Secretary of State.

Made, entered, and effective .

Lee Beyer

Chairman

John Savage

Commissioner **[*13]**

Ray Baum

Commissioner

A person may petition the Commission for the amendment or repeal of a rule pursuant to ORS 183.390. A person may petition the Court of Appeals to determine the validity of a rule pursuant to ORS 183.400.

APPENDIX A

ORDER NO. 04-012

Customer Proprietary Network Information

860-032-0510
Customer Proprietary Network Information (CPNI)

(1) The purpose of this rule is to specify requirements under which telecommunications carriers may use, disclose, or permit access to customer proprietary network information. This rule does not relieve telecommunications carriers of any requirements imposed by the Federal Communications Commission (FCC) regarding Customer Proprietary Network Information in 47 Code of Federal Regulations (CFR), Part 64, § 64.2001 through § 64.2009, or by Section 222 of the Communications Act of 1934, as amended (47 USC 222).

(2) This rule applies to all telecommunications carriers providing intrastate telecommunications service in Oregon, except that it applies to telecommunications cooperatives only for services which are subject to the Commission's jurisdiction pursuant to ORS 759.220 and ORS 759.225. [*14]

(3) For purposes of this rule, the following definitions apply:

(a) "Aggregate customer proprietary network information" or "Aggregate CPNI" means collective CPNI data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(b) "Carrier" or "telecommunications carrier" means any provider of intrastate telecommunications service as defined in ORS 759.005(2). "Carrier" or "telecommunications carrier" includes competitive providers, telecommunications cooperatives, and telecommunications utilities.

(c) "Customer" means a subscriber, end-user, or consumer of carrier services or an applicant for carrier services.

(d) "Customer proprietary network information" or "CPNI" means individual customer information that a carrier accumulates in the course of providing telecommunications service to the customer. CPNI includes information that relates to type, quantity, technical configuration, destination, location, billing amounts, and usage data. CPNI also includes information contained in bills pertaining to telecommunications service received by a customer, except that CPNI does not include subscriber list [*15] information.

(e) "Subscriber list information" means the listed names of subscribers of a carrier and those subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of establishment of service), or any combination of such listed names, numbers, addresses, or classifications.

(4) Except as required by law or with approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of telecommunications service shall only use, disclose, or permit access to CPNI in its provision of:

(a) The telecommunications service from which such information is derived; or

(b) Services necessary to, or used in, the provision of such telecommunications

service, including publishing of directories and billing.

(5) A telecommunications carrier shall disclose CPNI, upon affirmative written request by the customer, to any person designated by the customer.

(6) A telecommunications carrier that obtains CPNI by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate CPNI for any lawful purpose. However, a [*16] telecommunications carrier may use, disclose, or permit access to aggregate CPNI other than for purposes described in subsection (4) of this rule only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions, upon reasonable request therefor.

(7) Nothing in this rule prohibits a telecommunications carrier from using, disclosing, or permitting access to CPNI obtained from its customers, either directly or indirectly through its agents:

(a) To initiate, render, bill, or collect for telecommunications services;

(b) To protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; or

(c) To provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer.

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 756.040, 759.015 & 759.030

Hist.: New

Carrier to Carrier Transactions

860-032-0520
Customer Service Records (CSRs)

(1) The purpose of this rule is to provide for an exchange of information, [*17] in order to ensure that a requesting Local Service Provider (LSP) has enough customer information from the current LSP, so a customer can migrate local exchange service from one LSP to another in a seamless and timely manner, without delays or unnecessary procedures. This rule does not relieve carriers of any requirements imposed by either the Federal Communications Commission (FCC) regarding Customer Proprietary Network Information in 47 Code of Federal Regulations (CFR), Part 64, § 64.2001 through § 64.2009, or by Section 222 of the Communications Act of 1934, as amended (47 USC 222).

(2) This rule:

(a) Applies to telecommunications carriers without an approved interconnection agreement with the requesting LSP that addresses requirements covered by this rule.

(b) Does not apply to telecommunication cooperatives.

(c) Does not apply to telecommunications carriers with an interconnection

agreement with the requesting LSP, which is approved pursuant to OAR 860-016-0020 through 860-016-0030, that addresses requirements covered by this rule.

(3) For purposes of this rule, the following definitions apply:

(a) "Carrier" or "telecommunications carrier" [*18] means any provider of intrastate telecommunications service as defined in ORS 759.005(2). "Carrier" or "telecommunications carrier" includes competitive providers and telecommunications utilities.

(b) "Circuit ID" means circuit identification number of a loop.

(c) "Commission" means the Public Utility Commission of Oregon.

(d) "Competitive local exchange carrier" or "CLEC" means a competitive provider as defined in OAR 860-032-0001 that provides local exchange service.

(e) "Customer" means a subscriber, end-user, or consumer of local exchange services or an applicant for local exchange services.

(f) "Customer service record" or "CSR" means the customer's account information, which includes the customer's address, features, services, and equipment.

(g) "Customer proprietary network information" or "CPNI" has the meaning given in OAR 860-032-0510.

(h) "Current LSP" means the LSP from whom a customer receives local exchange service prior to migrating to another LSP. After migration occurs, the current LSP becomes the customer's old LSP.

(i) "Local exchange service" has the meaning given in OAR 860-032-0001.

(j) "Local service provider" or "LSP" means the carrier that interacts directly [*19] with the customer and provides local exchange service to that customer. Based on the service configuration, an LSP can also be the NSP. In some cases, the following more specific designations may be used:

(A) "New local service provider" or "new LSP" means the new local service provider after service migration occurs.

(B) "Old local service provider" or "old LSP" means the old local service provider after service migration occurs.

(k) "Local service request" or "LSR" means the industry standard forms and supporting documentation for ordering local exchange services.

(l) "Network service provider" or "NSP" means the company whose network carries the dial tone, switched services and loop(s) to the customer. Based on the service configuration, a NSP can also be the LSP. In some cases the following more specific designations may be used:

(A) "Network service provider-switch" or "NSP-switch" means the provider that provides the dial tone and switched services.

(B) "Network service provider-loop" or NSP-loop" means the provider of the local loop to the end user premises or other mutually agreed upon point.

(C) "New network service provider" or "new NSP" means the new network service provider [*20] after service migration occurs.

(D) "Old network service provider" or "old NSP" means the old network service provider after service migration occurs.

(m) "Requesting LSP" means the LSP whom a customers has authorized to view his/her customer service information. After migration occurs, the requesting LSP becomes the customer's new LSP.

(n) "Resale" means the sale of a local exchange telecommunications service by a CLEC to a customer by purchasing that service from another carrier.

(o) "Transition information" means network information (e.g., circuit ID), identity of the current network service providers (e.g., loop and switch providers), and identity of other providers of services (e.g., E-911 provider, directory service provider) associated with a customer's telecommunications service.

(p) "UNE" means unbundled network element. The following more specific designations may be used.

(A) "UNE-loop" or "UNE-L" means unbundled network element loop.

(B) "UNE-platform" or "UNE-P" means unbundled network element platform.

(4) An LSP may request CSR information for a specific customer from the customer's current LSP. Before requesting a CSR for a specific customer, the requesting LSP must [*21] have on file one of the following verifiable forms of customer authorization:

(a) Letter of authorization from the customer to review his/her account;

(b) Third party verification of the customer's consent;

(c) Recording verifying consent from the customer to review his/her account; or

(d) Record of oral authorization given by the customer, which clearly gives the customer's consent to review his/her account.

(5) Every requesting LSP shall retain the customer authorization on file for one year from the date it received such authorization.

(6) A customer's current LSP may not require a copy of the end user's authorization from the requesting LSP prior to releasing the requested CSR. In the event the customer complains or other reasonable grounds exist, the current LSP may request verification of the customer's authorization from the requesting LSP. The parties must attempt to resolve any dispute concerning the validity of the customer's authorization prior to filing a formal complaint with the Commission.

(7) When requesting a CSR, a requesting LSP:

(a) Shall include, at a minimum, the following information:

(A) Customer's telephone number(s);

(B) An indication of customer consent [*22] to review the CSR;

(C) How to respond with the CSR information;

(D) The name of the requesting LSP, with contact name and telephone number, for questions about the request;

(E) Date and time the request was sent;

(F) Indication whether circuit ID is requested for UNE-L reuse; and

(G) Indication whether listing information is requested.

(b) May include the following information:

(A) Customer service address;

(B) Customer name;

(C) Tracking number for the request; or

(D) Other applicable information.

(8) Requesting LSPs may transmit CSR requests via facsimile, electronic mail, regular mail, or other agreed-upon means. All carriers must, at a minimum, allow for reception of CSR requests via facsimile.

(9) All carriers should reuse existing UNE-L facilities in lieu of ordering a new UNE-L. A UNE-L shall be considered reusable when the existing circuit or facilities are no longer needed by the old LSP to provide service to the migrating customer or any customer that is currently using those facilities. When requested and reuse of the UNE-L facility is available the current LSP must provide the circuit ID for the requested UNE-L facility to the requesting LSP as part of the CSR response [*23] or transition information. Authorization is not required from the old LSP for the new LSP to reuse portions of the network that were provided to the old LSP by a NSP(s), and the old LSP shall not prohibit such reuse. To order the reuse of a UNE-L facility, the new LSP shall furnish the circuit ID on the LSR issued to the existing or new NSP-L.

(10) When responding to a CSR request the current LSP shall provide, at a minimum, the following:

(a) Account level information, including the following:

(A) Billing telephone number and/or account number;

(B) Complete customer billing name and address;

(C) Directory listing information including address and listing type, when requested;

(D) Complete service address (including floor, suite, unit); and

(E) Requesting LSP's tracking number when provided on the CSR request.

(b) Line level information, including the following:

(A) Working telephone number(s);

(B) Current preferred interexchange carrier(s) (PIC) for interLATA and intraLATA toll, including PIC freeze status;

(C) Local freeze status;

(D) All vertical features (e.g., custom calling, hunting) identified in a manner that clearly designates the products and services to which the customer [*24] subscribes;

(E) Options (e.g., Lifeline, 900 blocking, toll blocking, remote call forwarding, off-premises extensions), if applicable;

(F) Service configuration information (e.g., resale, UNE-L, UNE-P);

(G) Identification of the NSPs and/or LSPs, when different from the LSP providing the response. This is considered transition information;

(H) Identification of data services or any other services on the customer's line utilizing that UNE-L (e.g., alarm services); and

(I) Circuit ID to be provided when requested and the UNE-L is not being used for other services. This is considered transition information.

(11) If requested, and not provided with the CSR response, the current LSP shall provide transition information, and identify the current provider(s) of various service components to the customer (e.g., loop, directory service) if different from the current LSP. Circuit ID should only be provided by the current LSP when the UNE-L is reusable.

(12) Current LSPs responding to CSR requests may transmit the CSR information by facsimile, electronic mail, electronic data interexchange, or by other agreed-upon means. All carriers must, at a minimum, allow for transmission of responses to [*25] CSR requests by facsimile. Regular mail may be used if the response is 50 or more pages or if the CSR request was transmitted by regular mail.

(13) Upon the effective date of this rule, current LSPs shall respond to CSR requests within two business days of when the request was received. Six months after the effective date of this rule, current LSPs shall respond to CSR requests within one business day of when the request was received. If the current LSP cannot meet the response requirement for any legitimate reason, such as complex services, the current LSP shall notify the requesting LSP within 24 hours of when the request was received. The notification shall include a legitimate reason for the delay. The current LSP and the requesting LSP shall negotiate in good faith to establish a reasonable time for the current LSP to respond to the request.

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 756.040, 759.015 & 759.030

Hist.: New

DIVISION 035

[EDITOR'S NOTE: TEXT WITHIN THESE SYMBOLS [O> <O] IS OVERSTRUCK IN THE SOURCE.]

[O>OPEN NETWORK ARCHITECTURE (ONA) FOR TELECOMMUNICATIONS PROVIDERS<O]

860-035-0010
[O>Purpose and Applicability

(1) The purpose of this division [*26] is to prescribe the Open Network Architecture (ONA) environment within the State of Oregon in order to:

(a) Stimulate enhanced services availability to the public through the local exchange network;

(b) Foster development of innovative applications for ONA services and vigorous competition among all enhanced service providers;

(c) Encourage public use of enhanced services;

(d) Create a regulatory framework which ensures nondiscriminatory access to the local exchange network for all providers of enhanced services on equal rates, terms, and conditions; and

(e) Prescribe conditions under which local exchange carriers may furnish enhanced services in competition with other providers of enhanced service without undue competitive advantage.

(2) This division shall apply to all LECs operating within the State of Oregon with the following exceptions:

(a) LECs which are cooperatives, unincorporated associations, or telecommunications utilities serving less than 50,000 access lines in Oregon and not affiliated or under common control with any other kind of public utility providing service in Oregon are exempt from OAR 860-035-0030, 0040, 0060(1), 0070(1), 0080(4), and 0090(2) and (3);

(b) This [*27] division shall apply to LECs which are cooperatives or unincorporated associations only for services which are subject to regulation by the Commission pursuant to ORS 759.220 and ORS 759.225.

(3) A LEC, at its discretion, may elect to offer enhanced services solely on a structurally separated basis by means of LEC affiliates. Should a LEC make such an election, the LEC shall treat the LEC affiliates as customers.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852); PUC 12-1999, f. & ef. 11-18-99 (Order No. 99-709)

860-035-0020
[O>Definitions for Open Network Architecture

For purposes of this division:

(1) "Access Element (AE)" means an unbundled component of a BSA.

(2) "Aggregate CPNI" means summarized or aggregate noncustomer specific CPNI.

(3) "Ancillary Service (ANS)" means a service, such as billing and collection service or Operations Support Systems (OSS), which is performed by a local exchange carrier to directly administer or support provision of the LEC's basic and enhanced services. ANSs do not include the provision of common administration such as human resources, accounting, purchasing, [*28] inventory control, or other similar functions.

(4) "Basic Service" means a service which provides transmission capacity for the movement of information. Basic services include data processing, computer memory or storage, switching techniques and other activities which facilitate the movement of information.

(5) "Basic Service Element (BSE)" means an optional feature or function provided by a LEC as part of basic services. An optional feature or function can also be classified as a CNS.

(6) "Basic Serving Arrangement (BSA)" means basic services provided by a LEC which link customers to and through the LEC's network.

(7) "Building Block" means an element or group of elements representing the smallest feasible level of unbundling capable of being tariffed and offered as a service.

(8) "Collocation" means a service, offered by a LEC, which provides for placement and installation of a customer's equipment, software, and databases on LEC premises. Premises include central offices, remote network facilities, or any other similar location owned by the LEC. The equipment, software, and databases are owned by the customer.

(9) "Complementary Network Service (CNS)" means an optional feature [*29] or function provided by a LEC as part of basic services. An optional feature or function can also be classified as a BSE.

(10) "Comparably Efficient Interconnection (CEI)" means the provisioning of interconnection and network functionalities to customers and the LEC's own operations under the same rates, terms, and conditions, and on an unbundled and functionally equivalent basis.

(11) "Customer" means a subscriber, user, or consumer of LEC services or an applicant for LEC services.

(12) "Customer Proprietary Network Information (CPNI)" means individual customer data which a LEC accumulates in the course of providing basic services to the customer. CPNI includes types, quantities, and locations of services, billing amounts, repair information, calling patterns, and usage data. CPNI does not include listed name, address and telephone number, billed name, address, and telephone number, credit information, or information pertaining to enhanced or unregulated services supplied by a LEC.

(13) "Enhanced Service" means a service which employs computer processing applications that act on the format, content, code, protocol or similar aspects of the

customer's transmitted information; provides [*30] the customer with additional, different, or restructured information; or involves customer interaction with stored information. Enhanced services include but are not limited to information retrieval services, voice messaging, and protocol translation between customer equipment or software.

(14) "Enhanced Service Provider (ESP)" means a person which supplies enhanced services by using ONA services furnished by a LEC, including the enhanced services operation of a LEC and an IXC acting as an ESP. An IXC acts as an ESP only when it provides enhanced services to customers separate from its provision of basic services.

(15) "Interexchange Carrier (IXC)" means a provider of basic services, except extended area service, between local exchanges.

(16) "Joint Marketing" means the offering of enhanced and basic services by a LEC to customers either through contact initiated by the LEC or through contact initiated by the customer.

(17) "LEC Affiliate" means a person separate from the LEC which is either an affiliated interest or another company in which the LEC owns a controlling interest.

(18) "Local Exchange Carrier (LEC)" means a telecommunications utility, unincorporated association, or cooperative [*31] corporation which provides basic services within the boundaries of exchange maps filed with and approved by the Commission, and provides basic service to nearby exchanges as part of extended area service. A LEC includes its employees and individuals under contract.

(19) "Nonstructural Safeguards" means measures to prevent unjust discrimination and cross-subsidy of a LEC's enhanced service operations from the LEC's basic services operations. These measures include accounting rules, service unbundling, imputation, service deployment requirements, joint marketing, and CPNI restrictions.

(20) "Open Network Architecture (ONA) Services" means Basic Serving Arrangements, Access Elements, Basic Service Elements, Complementary Network Services, Ancillary Services, Collocation, and Virtual Collocation as defined in this division.

(21) "Operations Support Systems (OSS)" means services which support various network operation functions such as service provisioning, performance monitoring, and maintenance. OSS can be classified as an ANS.

(22) "Person" includes individuals, joint ventures, partnerships, corporations and associations, and governmental entities, or their officers, employees, agents, [*32] lessees, assignees, trustees or receivers.

(23) "Structural Safeguards" means measures to prevent unjust discrimination and cross-subsidy of a LEC's enhanced service operations from the LEC's basic services operations by employing separate personnel and facilities for enhanced services or a separate LEC Affiliate for enhanced services.

(24) "Tariff(s)" means any document on file with the Commission which specifies rates, terms, and conditions for LEC services, including price lists and special contracts.

(25) "Unbundling" means disaggregation of a service into building blocks or groups of building blocks which are offered to customers as separate services.

(26) "Unhooking" means any activity by a LEC which encourages a customer or prospective customer of an ESP to switch to the LEC's version of the same or substantially similar enhanced service at the time the ESP's customer contacts the LEC to obtain basic services which are necessary for operation of the enhanced service.

(27) "Virtual Collocation" means a service, offered by a LEC, which provides for placement and installation of customer selected equipment, software, and databases on LEC premises. Premises include central offices, [*33] remote network facilities, or any other similar location owned by the LEC.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852); PUC 9-1997, f. & ef. 4-17-97 (Order No. 97-119); PUC 9-2001, f. & cert. ef. 3-21-01 (Order No. 01-248)

860-035-0030
[O>Extent of Unbundling

(1) In order to encourage the development of enhanced services and provide for a more competitive enhanced services market, LECs shall unbundle their local exchange and exchange access services subject to conditions provided in these rules.

(2) Unless otherwise ordered by the Commission, within six months following adoption of this rule, LECs shall create BSEs and CNSs by separating all optional features and functions from existing basic services in their intrastate local exchange and interexchange access tariffs.

(3) At least six months prior to offering any enhanced service, a LEC shall create ANSs by separating such services from existing basic services in their intrastate local exchange and interexchange access tariffs.

(4) BSEs, CNSs, and ANSs shall be offered to customers without requiring purchase of a BSA or any other service. [*34]

(5) LECs which currently offer an enhanced service shall comply with sections (3) and (4) above within six months following adoption of this rule.

(6) Nothing in this rule shall preclude a LEC from combining AEs, BSEs, CNSs, and ANSs in order to create additional services so long as the unbundled services are also offered to customers separately.

(7) The LECs shall unbundle BSAs into AEs, CNSs, and BSEs. The level, extent, and implementation of BSA unbundling will be determined by Commission order or as provided in section (8) below.

(8) The LECs shall submit tariffs, which unbundle BSAs into AEs, CNSs and BSEs.

(9) Customers shall be permitted to request AEs as part of the request process for ONA services according to 860-035-0070. LECs may elect to implement the

resulting new ONA service but will not be required to do so until the LEC has unbundled BSAs according to provisions in sections (7) and (8) above.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852); PUC 12-1999, f. & ef. 11-18-99 (Order No. 99-709)

860-035-0040
[O>Tariffing

(1) Tariff nomenclature and service descriptions for ONA [*35] services shall be as consistent as possible with those adopted by the Information Industry Liaison Committee (IILC). Each LEC shall maintain a separate section of either its local exchange or interexchange access tariffs containing a listing of all intrastate ONA services offered by the LEC, or shall maintain a separate ONA tariff containing such a listing. The separate ONA section or tariff shall refer to appropriate tariff sections and price lists for each ONA service and include a compatibility matrix. The compatibility matrix shall indicate which BSAs and AEs are compatible with each BSE, CNS, and ANS offered by the LEC.

(2) Optional features and functions may be classified by a LEC as either BSEs, CNSs, or both.

(3) ONA services shall be made available in all tariffs where applicable.

(4) When a BSA is unbundled under the provisions of 860-035-0030 (7), (8) and (9) the resulting services shall be tariffed as AEs, BSEs, and CNSs.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852)

860-035-0050
[O>Allocation of Costs

If a telecommunications utility, unincorporated association, or cooperative [*36] corporation offers an enhanced service, costs and revenues of the enhanced service shall be allocated to the utility's enhanced service operation in accordance with rules contained in OARs 860-027-0052, 860-034-0520, and 860-034-0740.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852)

860-035-0060
[O>Rates for ONA Services

(1) Rates for ONA services contained in a LEC's interexchange access tariffs shall be equal to rates charged for the same ONA services when they are offered in the

LEC's local exchange tariffs, unless there are regulatory policy or cost differences.

(2) Rates for ONA services shall be published in tariffs and shall be based on pricing policies determined by Commission order.

(3) Rates for collocation and virtual collocation may include elements for safety, security, floor space, power, maintenance and other relevant costs.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852)

860-035-0070
[O>Deployment of ONA Services

(1) LECs shall issue an annual report providing a three-year deployment [*37] projection of ONA services availability by market area. The annual report shall identify and fully describe the current capabilities of each wire center, all ONA services that have become available since the previous report, and all ONA services that the LEC expects to make available within the ensuing three years. A copy of the annual report shall be filed with the Commission. LECs shall mail the annual report to customers upon their request.

(2) Upon request, LECs shall make avail-able to customers references which provide the technical specifications of LEC interfaces that could affect customer premises equipment or the functions provided to customers for the purpose of providing enhanced services.

(3) All requests for ONA services shall be promptly evaluated by the LEC. A request to unbundle an existing service shall be considered a request for an ONA service.

(a) Each LEC shall establish an ONA service request process within six months following adoption of this rule and make information about such process available to customers upon request;

(b) The LEC shall inform the requesting customer whether the request is complete within 14 days of receiving the request. Within the 14 [*38] days, the LEC shall return an incomplete request to the customer together with a detailed explanation of deficiencies and directions for correcting such deficiencies;

(c) Schedules for implementing ONA services may deviate from these rules by mutual agreement between the LEC and the requesting customer;

(d) LECs must use the same process, criteria, and cost methods to evaluate ONA service requests from their own enhanced services operations as they use to evaluate requests from customers;

(4) Complete requests for ONA services other than collocation and virtual collocation shall be evaluated pursuant to the following requirements:

(a) The LEC shall provide a written response to the customer within 120 days of receipt. A status report shall be provided to the customer within 80 days of receipt;

(b) The LEC shall implement the request by offering the service in tariffs or by

special contract if the service is feasible based on currently available technology and forecasted demand is sufficient to allow the LEC to recover its cost. The LEC shall implement the request as soon as practical and in any event no later than 12 months following the receipt of the customer's request. Implementation [*39] of AEs is the only exception. AEs shall be implemented as prescribed in 860-035-0030 (7), (8), and (9).

(5) Complete requests for collocation and virtual collocation shall be evaluated pursuant to the following requirements:

(a) The LEC shall provide a written response to the customer within 45 days of receipt;

(b) The LEC shall implement the request as soon as feasible and in any event no later than 6 months of the receipt of the request;

(c) The LEC shall implement a request for collocation or virtual collocation by offering the service in tariffs or by special contract if there is sufficient space or capacity and all applicable requirements in 860-035-0080(5) and 860-035-0110 are met.

(6) A LEC which rejects a request for an ONA service shall inform the requesting customer of any alternative arrangements which will perform the same or similar function.

(7) LECs shall maintain a detailed record of all requests made by customers for ONA services. At minimum, such records shall contain the name of the requesting customer, the date of the request, the specific type of service requested, the LEC's planned and actual response dates, the criteria and cost methods used to evaluate the request, [*40] and the response of the LEC. Such records shall be subject to audit by the Commission and its staff.

(8) Disputes concerning requests for ONA services are subject to the complaint process in OAR 860-035-0130.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852)

860-035-0080
[O>Availability of ONA Services

(1) A LEC which offers enhanced services on either a deregulated or regulated basis shall charge or impute to its own enhanced services operation the same tariffed or price listed rates for ONA services that the LEC offers to its customers.

(2) LECs which offer ONA services shall not give any advantage to their own enhanced services operation or otherwise discriminate regarding service availability, ordering, provisioning, and repair or access to technical standards.

(3) LECs shall not impose use and user restrictions for ONA services except as authorized by the Commission.

(4) A LEC which offers enhanced services on either a deregulated or regulated basis

shall make billing and collection available as an ANS to ESPs which provide enhanced services in direct competition with comparable enhanced [*41] services provided by the LEC at rates, terms, and conditions which are equivalent to rates, terms and conditions available to the LEC's enhanced service operations. LECs shall also offer to ESPs information which the LEC can capture in the LEC's network which ESPs could use to bill for enhanced services.

(5) A LEC which offers enhanced services on either a deregulated or regulated basis shall make any OSS service defined as an ONA service under federal law available as an ANS to customers, pursuant to OAR 860-035-0070(1), (2), (3), (6), (7), and (8). All customer requests for OSS services not defined as ONA services under federal law must be approved by the Commission unless there is a mutual agreement between the LEC and the requesting customer.

(6) All facilities connected to, or interacting with, the facilities of a LEC shall be operated in a manner which will not impede the LEC's ability to meet standards of service required in OARs 860-023-0055 and 860-034-0360. All LECs shall report situations contrary to this requirement promptly to the Commission.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order **[*42]** No. 93-852)

860-035-0090
[O>Access to CPNI

(1) Except as provided by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information (CPNI) by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of:

(a) The telecommunications service from which such information is derived, or

(b) Services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in section (1) of this rule. A local exchange carrier may use, disclose, or permit access to aggregate customer information other than [*43] for purposes described in section (1) of this rule only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefore.

(4) Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents:

(a) To initiate, render, bill, and collect for telecommunications services;

(b) To protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; or

(c) To provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service.

(5) Notwithstanding the other requirements of this section, a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service [*44] on a timely and unbundled basis, under non-discriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(6) A telecommunications carrier shall release a customer's CPNI to a third party only after the customer has authorized the telecommunications carrier to release such CPNI to the third party. A third party is any person other than the customer and the telecommunications carrier. A telecommunications carrier Affiliate is a third party.

(7) Each Oregon regulated telecommunications carrier shall specifically state in its tariffs the terms and conditions for providing CPNI and Aggregate CPNI.

(8) The term "telecommunications carrier" in this rule means any provider of "telecommunications service" as defined in ORS 759.005 (2)(g).

(9) The term "subscriber list information" means:

(a) Identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(b) [*45] That the carrier or an affiliate has published, or accepted for publication in any directory format.<O]

Stat. Auth.: ORS Ch 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852); PUC 5-1997, f. & ef. 1-9-97 (temp) (Order No. 97-006); PUC 8-1997, f. & ef. 2-19-97 (amended temp) (Order No. 97-044); PUC 11-1997, f. & ef. 8-14-1997 (Order No. 97-233); PUC 12-1999, f. & ef. 11-18-99 (Order No. 99-709)

860-035-0100
[O>Joint Marketing

(1) Subject to conditions pro-vided in these rules, LECs shall be permitted to engage in joint marketing. As part of joint marketing, the LECs shall be allowed to use CPNI in accordance with 860-035-0090.

(2) LECs shall not engage in unhooking.

(3) Whenever LEC personnel provide information about enhanced services in the course of a customer contact involving basic services, the LEC shall advise the customer in an unbiased manner that similar enhanced services may be available from other providers. The LEC shall so advise customers before taking an order for an enhanced service.

(4) A customer who subscribes to a LEC's enhanced service shall have seven days to cancel without cost or penalty. The [*46] LEC shall inform customers of this right at the time the order is placed.

(5) LECs shall not use CPNI to create lists of prospective enhanced services customers for use in unsolicited direct sales such as telemarketing and direct mail except LECs may create such lists using the CPNI of any customer who has authorized the LEC to use the customer's CPNI for that purpose.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852)

860-035-0110
[O>Collocation and Virtual Collocation

(1) LECs shall offer collocation and virtual collocation to customers as provided in this rule.

(2) Software and database collocation shall be limited to facilities designed for external applications such as rapid delivery platforms, service nodes, or memory partitions. All requests for software and database collocation must be approved by the Commission unless there is mutual agreement for such collocation between the LEC and the requesting customer.

(3) A LEC shall require customers to meet the following collocation requirements:

(a) Collocation space shall not be accessible by the general public. Customers shall comply with [*47] all reasonable security requirements of the LEC. Customers shall permit LEC personnel to enter and inspect collocation space upon 24 hours' notice, and only in the presence of a customer representative, except that LEC personnel may immediately enter in the event of an emergency;

(b) Customers shall be responsible for the installation, operation, and maintenance of its own equipment. LECs may offer installation, operation, and maintenance services to customers. Equipment compatibility shall be the responsibility of the customer;

(c) Customers are required either to maintain comprehensive general liability insurance issued by a company qualified to do business in Oregon or provide evidence of self-insurance, in order to protect against death, personal injury and property damage, in an amount of not less than $ 1 million;

(d) Customers are required to indemnify the LEC in the event there is damage to LEC equipment or the LEC's security is compromised as a result of the customer's intentional misuse or negligence;

(e) Customers shall request collocation in writing. The request shall specify technical and space requirements.

(4) LECs shall meet the following collocation requirements: [*48]

(a) If a customer has complied with all collocation requirements specified in this Division, the LEC shall permit the customer to collocate without regard to the technology employed by the customer;

(b) A LEC shall maintain and control access to its facilities in accordance with industry standards for security and safety. A LEC shall permit access to a customer's collocated facilities by authorized representatives of the customer in accordance with said standards;

(c) A LEC shall be required to indemnify the collocated customer against death, personal injury and property damage caused by the LEC's intentional misuse or negligence;

(d) A LEC shall assign space for collocation on a first-come, first-served basis based on the date the LEC receives a collocation request. The LEC shall maintain records documenting requests for collocation;

(e) In the event a LEC states it does not have sufficient space to allow for collocation and the customer disputes the LEC's assertion, the Commission's staff shall inspect the proposed point of collocation to verify that there is a lack of space. If the Commission's staff verifies that space is not available, the LEC shall deny collocation to the customer [*49] and offer the customer virtual collocation and CEI arrangements;

(f) Expansion of the LEC's enhanced services operation shall not take precedence over existing written requests for collocation. In the event a LEC requires space for basic services which is otherwise occupied by a customer, the LEC shall give the customer at least 12 months' written notice to vacate. Customers shall vacate on a last-in, first-out basis or as mutually agreed by all affected parties. Customers so forced to vacate shall be offered virtual collocation and CEI arrangements;

(g) In the event it is necessary for a LEC to construct or modify existing space to collocate a customer, the LEC may require the customer to pay reasonable construction costs for the construction of segregated space in a LEC facility. Thereafter, the LEC may charge a monthly service charge for the use of the segregated space;

(h) LECs shall permit customers to monitor, test, and control the customer's collocated equipment either on site or remotely;

(i) LECs shall permit a customer to transmit information, including signaling and protocols, through the LEC's network without interference or manipulation;

(j) To the extent that a LEC provides [*50] enhanced services by means of computer software operating in a processor external to its central office switches, the LEC shall make available to customers the same interfaces which the LEC uses to enable communications between its switches and such external processor.

(5) A LEC shall require customers to request virtual collocation in writing. Requests shall specify which equipment, software, and databases the customer requires.

(6) LECs shall meet the following virtual collocation requirements:

(a) A LEC shall maintain and control access to its facilities in accordance with industry standards for security and safety. A LEC shall permit access for inspection purposes by authorized representatives of the customer in accordance with said standards;

(b) A LEC shall assign space for virtual collocation on a first-come, first-served basis based on the date the LEC receives a request. The LEC shall maintain records documenting requests for virtual collocation;

(c) In the event a LEC states it does not have sufficient space to allow for virtual collocation and the customer disputes the LEC's assertion, the Commission's staff shall inspect the proposed point of virtual collocation to verify [*51] that there is a lack of space. If the Commission's staff verifies that space is not available, the LEC shall deny virtual collocation to the customer and offer the customer CEI arrangements;

(d) Expansion of the LEC's enhanced services operation shall not take precedence over existing written requests for virtual collocation. In the event a LEC requires space for basic services which is otherwise occupied by a customer, the LEC shall give the customer at least 12 months' written notice to vacate. Customers shall vacate on a last-in, first-out basis or as agreed by all affected parties. Customers so forced to vacate shall be offered CEI arrangements;

(e) In the event it is necessary for a LEC to construct or modify existing space to virtually collocate a customer, the LEC may require the customer to pay reasonable construction costs;

(f) Equipment may be purchased by either the LEC or the customer. If the customer purchases the equipment, the customer must provide all equipment and software necessary for virtual collocation that it desires to be dedicated solely for its own use. The LEC will lease such equipment from the customer for $ 1 in each central office where the customer subscribes [*52] to virtual collocation. The LEC will be responsible for installation, maintenance and removal of such equipment. LECs shall permit customers to monitor, test, and control the virtually collocated equipment;

(g) LECs shall permit a customer to transmit information, including signaling and protocols, through the LEC's network without interference or manipulation;

(h) To the extent that a LEC provides enhanced services by means of computer software operating in a processor external to its central office switches, the LEC shall make available to customers the same interfaces which the LEC uses to enable communications between its switches and such external processor.

(7) Disputes concerning collocation and virtual collocation are subject to the complaint process in OAR 860-035-0130.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852); PUC 9-1997, f. & ef. 4-17-97 (Order No. 97-119); PUC 12-1999, f. & ef. 11-18-99 (Order No. 99-709)

860-035-0120
[O>Safeguards

(1) LECs which offer enhanced services shall be permitted to provide enhanced services on an integrated basis using nonstructural safeguards [*53] and nondiscrimination requirements provided in these rules. Accordingly, LECs shall be allowed to use common personnel and facilities to provide basic and enhanced services, including deregulated enhanced services. If an enhanced service of a LEC is exempt from regulation, costs and revenues of the enhanced service shall be allocated to the LEC's enhanced service operation pursuant to rules for regulated and nonregulated accounting set forth in OARs 860-027-0052, 860-034-0394, and 860-034-0740.

(2) If a complaint filed pursuant to ORS 756.500 alleges that a LEC has discriminated against competitors or has misallocated costs and revenues between enhanced and basic services, the Commission will investigate the complaint. If the Commission determines that the allegations in the complaint are substantiated, the Commission shall impose appropriate remedies, including but not limited to structural safeguards, ratemaking adjustments, termination of or restrictions on the LEC's enhanced service offerings.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852)

860-035-0130
[O>Dispute Resolution

(1) If a [*54] LEC denies a request for ONA services, the LEC shall advise the customer as to the specific reasons and provide the customer reasonable opportunity to resolve problems identified by the LEC. The customer or LEC may seek assistance from the Commission and its staff to resolve the dispute before filing a complaint under this rule.

(2) If a LEC rejects a customer's request for an ONA service, or if a customer is not satisfied with a LEC's response to such a request, the customer may bring a complaint before the Commission under ORS 756.500. If a complaint is filed based upon a rejection of a request for service, the Commission shall determine whether the requested ONA service is viable, as defined in OAR 860-035-0070(4)(b). If the complaint relates to the timeliness of the LEC's response, or the implementation schedule, rates, terms, or conditions of providing the service, the Commission shall determine the reasonableness of the LEC's actions or positions.

(3) If a LEC specifically rejects a customer's request for collocation or virtual collocation, or if the LEC's implementation schedule, rates, terms, or conditions for collocation or virtual collocation are considered unsatisfactory [*55] by the customer, the customer may bring a complaint before the Commission under ORS 756.500. A customer may also bring a complaint under ORS 756.500 if the customer is not satisfied with the Comparably Efficient Interconnection arrangements. The Commission shall determine whether collocation or virtual collocation should be allowed or, if applicable, whether alternative arrangements meet the CEI requirement. If the customer's complaint relates to implementation schedule, rates, terms, or conditions of collocation or virtual collocation, the Commission shall determine whether the LEC's action or position is justified.<O]

Stat. Auth.: ORS Ch. 183, 756 & 759

Stats. Implemented: ORS 183.335 & 756.040

Hist.: PUC 13-1993, f. & ef. 6-23-93 (Order No. 93-852)

KENNY C. GUINN
Governor

STATE OF NEVADA
PUBLIC UTILITIES COMMISSION OF NEVADA
1150 E. William Street
Carson City, Nevada 89701-3109
Policy (775) 684-6107 • Fax (775) 684-6110
Staff (775) 684-6101 • Fax (775) 684-6120
http://puc.state.nv.us

RURAL NEVADA
557 W. Silver Street, No. 207
Elko, Nevada 89801
(775) 738-4914 • Fax (775) 778-6928

SOUTHERN NEVADA OFFICE
101 Convention Center Drive, Suite 250
Las Vegas, Nevada 89109
(702) 486-2600 • Fax (702) 486-2595

May 30, 2006

American Civil Liberties Union of Nevada
Attn: Gary Peck, Executive Director
732 S. 6th Street
Las Vegas, NV 89101

Re: ACLU vs. Verizon Nevada
File: CCU-052606-02-AA

Dear Mr. Peck:

Thank you for advising the Public Utilities Commission about the problems you are having with Verizon of Nevada.

Please be advised that a review and investigation has been initiated in your behalf by the Consumer Division's staff. You will be advised of our findings as soon as the investigation has been completed. We normally aim for a 30-day turn around on written complaints, although this may not always be possible if the case is highly technical or if we have to request additional information from the company.

In a separate letter to Verizon of Nevada, we have asked that they do not contact or respond directly to you without getting prior approval from this office. Likewise, we request that you do not contact the company regarding this matter without first contacting this office.

When making inquiries about your complaint, please be sure to include the above-captioned file number in all your correspondence.

Sincerely,

Andie Arthurholtz
Compliance Investigator II

AA:aa

cc: Carson City PUC

KENNY C. GUINN
Governor

STATE OF NEVADA
PUBLIC UTILITIES COMMISSION OF NEVADA
1150 E. William Street
Carson City, Nevada 89701-3109
Policy (775) 684-6107 • Fax (775) 684-6110
Staff (775) 684-6101 • Fax (775) 684-6120
http://puc.state.nv.us

RURAL NEVADA
557 W. Silver Street, No. 207
Elko, Nevada 89801
(775) 738-4914 • Fax (775) 778-6928

SOUTHERN NEVADA OFFICE
101 Convention Center Drive, Suite 250
Las Vegas, Nevada 89109
(702) 486-2600 • Fax (702) 486-2595

May 30, 2006

American Civil Liberties Union of Nevada
Attn: Gary Peck, Executive Director
732 S. 6th Street
Las Vegas, NV 89101

Re: ACLU vs. AT&T
File: CCU-052606-01-AA

Dear Mr. Peck:

Thank you for advising the Public Utilities Commission about the problems you are having with AT&T.

Please be advised that a review and investigation has been initiated in your behalf by the Consumer Division's staff. You will be advised of our findings as soon as the investigation has been completed. We normally aim for a 30-day turn around on written complaints, although this may not always be possible if the case is highly technical or if we have to request additional information from the company.

In a separate letter to AT&T, we have asked that they do not contact or respond directly to you without getting prior approval from this office. Likewise, we request that you do not contact the company regarding this matter without first contacting this office.

When making inquiries about your complaint, please be sure to include the above-captioned file number in all your correspondence.

Sincerely,

Andie Arthurholtz
Compliance Investigator II

AA:aa

cc: Carson City PUC

STATE OF VERMONT
PUBLIC SERVICE BOARD

Docket No. 7192

Petition for Investigation into Alleged Unlawful)
Customer Records Disclosure by Verizon New)
England Inc., d/b/a Verizon Vermont)

Order entered: 6/27/2006

ORDER OPENING INVESTIGATION

INTRODUCTION

On June 21, 2006, the Department of Public Service ("Department") filed a Petition for Investigation into Alleged Unlawful Customer Records Disclosure by Verizon New England Inc., d/b/a Verizon Vermont ("Verizon"). In its Petition, the Department alleges that Verizon has not adequately responded to certain information requests from the Department made pursuant to 30 V.S.A. § 206. The Department states that Verizon's failure has hindered the Department's ability to discharge its statutory duty. As a result, the Department asks us to open an investigation, consolidate the investigation with Docket 7183 (in which the Public Service Board is considering a petition from eight ratepayers concerning Verizon's alleged disclosure of customer information to the National Security Agency), and impose penalties on Verizon.

The Department's Petition raises serious issues that we need to resolve. The ability to obtain information is critical to enable the Department to adequately perform its responsibilities. Accordingly, we will open an investigation into the Department's Petition.

At this time, however, we will not schedule a prehearing conference or establish a schedule. The Department has stated in Docket 7183 that it would seek to consolidate this investigation with that docket. We have established a schedule in Docket 7183 to address this issue as well as to consider a motion to dismiss that Verizon has stated that it intends to file. It is

reasonable to await our resolution of the consolidation issue and dispositive motions before holding a prehearing conference in this proceeding.[1]

ORDER

IT IS HEREBY ORDERED, ADJUDGED AND DECREED by the Public Service Board of the State of Vermont that:

1. Pursuant to 30 V.S.A. §§ 203, 209, 218(a), an investigation is commenced regarding Alleged Unlawful Customer Records Disclosure by Verizon New England Inc., d/b/a Verizon Vermont.

Dated at Montpelier, Vermont, this 27th day of June, 2006.

s/James Volz)
)
) PUBLIC SERVICE
)
s/David C. Coen) BOARD
)
) OF VERMONT
s/John D. Burke)

OFFICE OF THE CLERK

FILED: June 27, 2006

ATTEST: s/Susan M. Hudson
Clerk of the Board

NOTICE TO READERS: This decision is subject to revision of technical errors. Readers are requested to notify the Clerk of the Board (by e-mail, telephone, or in writing) of any apparent errors, in order that any necessary corrections may be made. (E-mail address: Clerk@psb.state.vt.us)

1. We intend to hold a status conference in Docket 7183 on August 23 to set the schedule after resolving the preliminary issues.

STATE OF VERMONT
PUBLIC SERVICE BOARD

Docket No. 7193

Investigation into Alleged Unlawful Customer)
Records Disclosure by AT&T Communications)
of New England, Inc.)

Order entered: 6/29/2006

ORDER OPENING INVESTIGATION AND NOTICE OF PREHEARING CONFERENCE

INTRODUCTION

On June 21, 2006, the Department of Public Service ("Department") filed a Petition for an Investigation into Alleged Unlawful Customer Records Disclosure by AT&T Communications of New England, Inc. ("AT&T"), a company providing intrastate communications in Vermont. The Petition alleges that the Department sought information from AT&T, pursuant to 30 V.S.A. § 206, regarding disclosure of customer information to the United States National Security Agency and any other state or federal agency. The Department further alleges that AT&T's response "does not even attempt to answer the specific questions posed" and that this has obstructed the Department's ability to discharge its statutory duties. The Department also alleges that AT&T is bound by state and federal laws applicable to disclosure of customer records to third parties for purposes other than connecting, tracking and billing for telephone calls. The Department asks this Board to open an investigation, to impose penalties on AT&T for failing to adequately respond to the Department's request and to order further relief that may be just and proper.

The Department's Petition raises serious issues that we need to resolve. The ability to obtain information is critical to enable the Department to adequately perform its responsibilities. Accordingly, we will open an investigation into the Department's Petition.

We note that similar issues have been raised in Docket No. 7183, Petition of Eight Ratepayers for an Investigation of Possible Disclosure of Private Telephone Records Without Customers' Knowledge or Consent by Verizon New England Inc., d/b/a Verizon Vermont, and also in Docket No. 7192, Petition for Investigation into Alleged Unlawful Customer Records Disclosure by Verizon New England Inc., d/b/a Verizon Vermont. We recognize that the similarity of the factual and legal issues presented in all three dockets may suggest the appropriateness of parallel schedules.

ORDER

IT IS HEREBY ORDERED, ADJUDGED AND DECREED by the Public Service Board of the State of Vermont that:

1. Pursuant to 30 V.S.A. §§ 203, 209, 218(a), an investigation is commenced regarding Alleged Unlawful Customer Records Disclosure by AT&T Communications of New England Inc.

2. Pursuant to 30 V.S.A. § 10, the Board will hold a prehearing conference in this matter on Wednesday, July 19, 2006, commencing at 10:00 A.M., at the Public Service Board Hearing Room, Third Floor, 112 State Street, Montpelier, Vermont.

Dated at Montpelier, Vermont, this 29th day of June, 2006.

s/James Volz)
)
) PUBLIC SERVICE
)
s/David C. Coen) BOARD
)
) OF VERMONT
s/John D. Burke)

OFFICE OF THE CLERK

FILED: June 29, 2006

ATTEST: s/Susan M. Hudson
Clerk of the Board

NOTICE TO READERS: This decision is subject to revision of technical errors. Readers are requested to notify the Clerk of the Board (by e-mail, telephone, or in writing) of any apparent errors, in order that any necessary corrections may be made. (E-mail address: Clerk@psb.state.vt.us)