BEFORE THE PUBLIC UTILITY COMMISSION

OF OREGON

UM 1265

AMERICAN CIVIL LIBERTIES UNION OF OREGON, Complainant, v. VERIZON NORTHWEST, INC., UNITED TELEPHONE COMPANY OF THE NORTHWEST, dba SPRINT, and QWEST CORPORATION, Defendants.	AMERICAN CIVIL LIBERTIES UNION OF OREGON'S REPLY TO RESPONSES OF QWEST, UNITED TELEPHONE COMPANY OF THE NORTHWEST D/B/A EMBARQ, AND VERIZON NORTHWEST, INC.

The American Civil Liberties Union of Oregon ("ACLU") submits this Reply to the responses filed by Qwest, United Telephone Company of the Northwest ("United"), and Verizon Northwest, Inc ("Verizon"). The ACLU renews its request, pursuant to OAR 860-013-0015, that the Public Utility Commission ("Commission") conduct a thorough investigation into Oregon telecommunications companies' handling of legally-protected customer information and communication contents. As part of its investigation, the Commission should learn exactly what

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

customer information Oregon telecommunications companies collect about Oregon intra-state communications—whether local calls, toll calls, e-mail, or other communications. And the Commission should require each telecommunications company to disclose in what situations, and under what authority, it has disclosed or would disclose customer information or the contents of any communications to any other person or entity, government or private.

Despite Verizon's efforts to confuse the Commission and inject issues involving international terrorism, the issues raised by the ACLU are of a more local and domestic nature. Simply put, the citizens of Oregon want to know whether telecommunications companies doing business in Oregon, and thus regulated by the Commission, provided intra-state telephone call information to any person or entity, and if they did, under what authority.

A. <u>The Commission Has Jurisdiction Over State Law and Regulation</u>.

The Commission's jurisdiction over telecommunications companies doing business in Oregon is readily obvious. However, Verizon attempts to avoid an investigation of its conduct within the State of Oregon by asserting in its response that the Commission should not investigate this matter because federal law—in certain, specific circumstances—both authorizes telecommunications companies to disclose information to federal government agencies and in some cases prohibits the companies from disclosing whether or not they have complied with, or even received, properly-formed government requests. The ACLU does not dispute that, if proper procedures have been followed, certain disclosures of limited customer information to specified federal government entities may be appropriate and protected under federal law. However, federal telecommunications law has never been held to preempt all state law and regulation in the field of telecommunications. Therefore, in the absence of controlling federal

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

telecommunications law, state law applies. Because the Commission has both jurisdiction over state regulations and broad power to investigate telecommunications companies under ORS Chapter 756, it is wholly appropriate for it to do so in this matter.

1. Congress has not displaced state telecommunications regulation.

Because Congress has not "occupied the field" of intra-state telecommunication regulation, state law applies to the extent it does not actually conflict with federal law. The leading case of *Silkwood v. Kerr-McGee Corp.*, 464 U.S. 238 (1984), summarizes the two types of federal preemption principles, "field preemption" and "conflict preemption":

> [S]tate law can be preempted in either of two general ways. If Congress evidences an intent to occupy a given field, any state law falling within that field is preempted. If Congress has not entirely displaced state regulation over the matter in question, state law is still preempted to the extent it actually conflicts with federal law . . . .

Id. at 248 (citations omitted). No case points to field preemption regarding telecommunications regulation. In fact, the federal Telecommunications Act of 1996 expressly preserves state regulatory authority via its preemption provision: "Nothing in this section shall affect the ability of a State to impose . . . requirements necessary to preserve and advance universal service, protect the public safety and welfare, ensure the continued quality of telecommunications services, and safeguard the rights of consumers." 47 U.S.C. § 253(b) (2000). By including this provision, Congress has shown a clear intent not to occupy the field of telecommunications regulation. Therefore, state telecommunications law is only preempted to the extent that it actually conflicts with federal law.

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

2. State law applies when a telecommunications company does not comply with the strict procedures and limits of any federal statute.

Because state regulation is valid and consistent with Congress's intent, the next inquiry is whether the express federal statutes that Verizon cites in its response preempt state law or otherwise insulate telecommunications companies from investigation by the Commission. The ACLU does not dispute that, where applicable, federal law may preempt state law. However, because federal statutes that allow for disclosure of customer information include strict limits on the scope of that information and prescribe strict procedures for its disclosure, it is appropriate and necessary for the Commission to investigate whether Oregon telecommunications companies violated state law.

In its response, Verizon cites several federal statutes to support its claim that the Commission cannot investigate whether it disclosed customer information in violation of Oregon law or regulation.[1] Each of the statutes Verizon cites contains either specific procedures under which information may be disclosed, specific limits on what information may be disclosed, or both. For example, 18 U.S.C. § 2511(2)(a)(ii) allows telecommunications companies to assist "persons authorized by law" to conduct wiretaps *only* when the company has received either

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

18 U.S.C. § 2511(2)(a)(ii) (2000).

---

[1] Specifically, Verizon refers to 18 U.S.C. §§ 2511(2), 2511(3), 2518(7), 2702(b), 2702(c), 2709 and 50 U.S.C. §§ 1805(f), 1805(i), 1843. Those statutes are attached as Exhibit 1.

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

In either case, the authorization must "set[] forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specify[] the information, facilities, or technical assistance required." *Id.* The Commission should also note that nothing in this statute prohibits a telecommunications company from disclosing whether it received an authorization or disclosed information pursuant to an authorization. Nor does the statute otherwise insulate a company from making such disclosures when compelled to do so by state authority. Therefore, it is appropriate for the Commission to investigate whether any Oregon telecommunications company has disclosed customer information under this statute and whether it strictly complied with the statutes' requirements when it has disclosed information.

Verizon also references 18 U.S.C. § 2709, which requires a telecommunications company to turn over certain information if it receives a national security letter ("NSL") and purports to prohibit the company from disclosing whether or not it has received such a letter. This statute, however, contains three important limitations. First, the information that can be provided is limited to the "name, address, length of service, and local and long distance toll billing records" of the object of a national security letter. 18 U.S.C. §§ 2709(b)(1)–(2) (2000). Second, a single NSL can request information of only one "person or entity." *Id.* Third, only certain government officials may request telecommunications using a NSL, namely "[t]he Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office . . . ." *Id.* at § 2709(b). Further, that official must "certif[y] in writing" that the "records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." *Id.* To the extent

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

that any telecommunications company provided information in excess of the statutory limitations, provided the information of more than one person or entity under each request, or provided information in response to an NSL that lacked proper credentials or certification, it cannot seek protection of the federal statute if its disclosures violate state law. Therefore, the Commission has jurisdiction and authority to determine whether any disclosures made under color of 18 U.S.C. § 2709 strictly comply with the statutory language and if not, to determine whether such disclosures violate state law or regulation.[2]

Although Verizon's response mentions other statutes in passing, it does not discuss them in detail. Neither will this Reply, except to point out that all of the statutes have either strict limits on the scope of information that can be turned over, strict procedures for its disclosure, or both. To the extent that any telecommunications company failed to comply with the strictures of each statute, the Commission should investigate whether any disclosures were made in violation of state law.

/ / /

[2] The ACLU is not asking the Commission to investigate any federal government anti-terrorism efforts nor is the ACLU seeking an investigation of whether any telecommunications companies disclosed international telephone information to any government or entity. Rather, the ACLU is solely seeking an investigation of whether telecommunications companies doing business in Oregon complied with Oregon law, whether they provided customer information to any person or entity and if they did, under what authority.

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

3. The telecommunications companies can disclose whether they provided customer information to any person or entity.

With the exception of 18 U.S.C. § 2709(c), none of the statutes referenced in Verizon's response purport to limit a telecommunications company's ability to disclose whether or not it received a request for information under a statute or otherwise complied with statutory provisions.

Verizon did not directly invoke the protection of § 2709(c) in its response, though even if it had attempted to do so, the statute's language cannot prevent a properly instigated state investigation from determining whether a telecommunications company has violated state law or regulation by disclosing information that exceeds the scope of or does not otherwise comply with the federal statute.

Section 2709(c) states, in relevant part, "[n]o wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section." 18 U.S.C. § 2709(c) (2000). A recent amendment to the statute, however, allows for judicial review of both the scope of information requested under an NSL and of the terms and conditions of nondisclosure imposed on a recipient of letter. *See* USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, 211 (Mar. 9, 2006) (codified at 18 U.S.C. 3511) (hereinafter "Reauthorization Act").[3] This change was likely a response to judicial scrutiny indicating Fourth Amendment concerns about the previous version of the statute's lack of judicial review.[4]

---

[3] The Reauthorization act is retroactive. *See Doe I v. Gonzales*, 449 F.3d 415, 418-419 (2d Cir. 2006).

[4] At least two courts have expressed concern that the nondisclosure provisions of §

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

Under the amended law, any telecommunications company that receives or has received an NSL can petition a United States district court to rule on the validity of the request for information. Reauthorization Act, 18 U.S.C. § 3511(a), 120 Stat. 211 (2006). The court can also amend any NSL if it determines that the request for information would be "unreasonable, oppressive, or otherwise unlawful." *Id.* Therefore, it follows that if a telecommunications company receives an NSL that requests information in excess of what is authorized by statute or that does not comply with the statute's procedural requirements, it has both the option and the duty to petition a federal court to bring the order into compliance with federal law. If the company chooses not to petition a federal court and subsequently releases information in excess of what is authorized by statute (or releases information pursuant to a letter that does not comply with the statute's procedures), then the company, to the extent that its disclosures violate state law or regulation, cannot seek protection under 18 U.S.C. § 2709(c) from a state investigation of the state law violation.

Because Congress has expressly said that it has not occupied the field of telecommunications regulation, state law applies whenever the specific limits and procedures of federal telecommunications statutes are exceeded. Except to the extent that telecommunications companies complied with the limits and procedures of a federal statute, any disclosure by them of customer information or communications content is governed by state law. And where a state agency has

---

2709 violate the First Amendment. *Doe v. Ashcroft*, 334 F. Supp.2d 471, 526-27 (S.D.N.Y. 2004) (remanded by *Doe I*, 449 F.3d at 419, to reconsider First Amendment issue in light of the Reauthorization Act.); *Doe v. Gonzales*, 386 F. Supp.2d 66, 78-82 (D. Conn. 2005) (Appeal dismissed by *Doe I*, 449 F.3d at 421, after the Government dropped its opposition to plaintiff's revelation that he had received a NSA.). While the Commission need not reach this issue, it is noteworthy that the statute's constitutionality, even as amended, is still in question.

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

properly initiated an investigation into a phone company's activities, federalism principles dictate that the agency must be able to determine whether the company fully complied with federal law in order to determine whether the company has violated non-preempted state laws.

B. Private Companies May Not Assert the "State Secrets" Privilege.

Although Verizon asserts its belief that the United States Government will take steps to prohibit the disclosure of information by the telecommunications companies, the United States has not done so in this matter, and it is unclear whether it would have any basis to do so. Again, the ACLU does not dispute that telecommunications companies may make certain, limited disclosures to the federal government in strict compliance with federal law. And, although the United States may assert certain evidentiary privileges to prevent certain disclosure of information that could threaten national security, it is not clear that it may do so to prevent a state entity from investigating state law violations.

It is important to note that the United States has not intervened in this matter. That is crucial because 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." *U.S. v. Reynolds,* 345 U.S. 1, 7 (1953). Because the United States has not intervened in this matter, it is not appropriate to dismiss the ACLU's complaint based on hypothetical situations nor does the Commission even need to consider Verizon's state secrets claims. Only if the United States seeks leave to intervene under OAR 860-012-001, and if the Commission allows intervention, will the Commission need to determine whether the United States can assert any claimed privileges in a state administrative proceeding concerning state law and regulatory violations.

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

C. Verizon's Suggestion that the Commission Dismiss the ACLU's Request Because of Other State and Federal Proceedings is Misguided.

In its response, Verizon urges the Commission to reject the ACLU's request because the Federal Communications Commission ("FCC") and a handful of state agencies have declined to review telecommunications company activities in their respective jurisdictions. The Commission should reject this suggestion because the determinations of other agencies are inappropriate bases for analyzing issues involving Oregon law and regulatory claims. In addition, each of the state and federal determinations that Verizon cites is readily distinguishable from this matter.

Verizon claims that other state commissions deciding whether to entertain similar ACLU complaints have unanimously declined to do so. This is false. Both the Nevada Public Utilities Commission and the Vermont Public Service Board have initiated investigations. *See* Letters from Andie Arthurholtz, Nevada Compliance Investigator to Gary Peek, Executive Director, ACLU of Nevada (May 30, 2006) (attached as Exhibits 2 and 3); Vermont Orders Opening Investigation of Verizon and AT&T dated June 27, 2006 (attached as Exhibits 4 and 5). Regarding the Vermont matter, Dan O'Brien, Vermont's Commissioner of Public Service, stated, "It is sometimes the job of the states to make sure the federal government, or these companies at the request of the federal government, don't cross certain lines." Louis Porter, *State Orders Inquiry Into Phone Records Flap*, RUTLAND HERALD (June 3, 2006) (attached as Exhibit 6). In other states, the decisions of appropriate administrative bodies are still pending. Maine, Connecticut, and Washington, among others, are still reviewing complaints under their own state laws and regulations.

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

Verizon additionally comments that the Commission should reject the ACLU's request for an investigation because the FCC has rejected a request to investigate the telecommunications companies' activities due to the classified nature of the NSA's activities. The FCC's refusal to investigate should have no bearing on whether the Commission conducts its own investigation, because (1) the FCC is a federal agency, acting under federal law, and its determinations are not conclusive as to whether the companies violated Oregon law and regulations, and (2) as a federal agency, the FCC may be less willing to challenge activities that potentially involve another federal agency. Therefore, the Commission should grant the ACLU's request for an investigation into Oregon law violations despite (or perhaps because of) the FCC's failure to conduct an inquiry into possible federal law violations.

Verizon's notation that four states—Delaware, Iowa, Virginia, and New York—have declined to conduct investigations also misses the mark. The material provided by Verizon covering each of those matters reveals that those states' determinations were specific to the laws of each state. First, Delaware has not declined to investigate, but has merely decided to wait six months for resolution of any federal issues before deciding whether to initiate its own investigation. Second, the Iowa Utilities Board declined to investigate because Iowa has deregulated the telecommunications industry, therefore the Board determined that it did not have jurisdiction to investigate under Iowa Code § 476.1D(1). *See* Letter from David Lynch, General Counsel, Iowa Utils. Board, Verizon Response Exhibit 4. Third, the Virginia State Corporation Commission declined to investigate because the complaint did not identify any Virginia law or regulation that prohibited Verizon's alleged conduct. *See* Letter from William H. Chambliss, General Counsel, Virginia State Corporation Commission, Verizon Response

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

Exhibit 3. Finally, the New York Department of Public Service likewise declined to investigate because they determined that there was no New York law or administrative rule that prohibited Verizon's alleged conduct. *See* Letter from William M. Flynn, Chairman, New York Public Utilities Commission, Verizon Response Exhibit 2.

As noted in the ACLU's original request for an investigation, the Oregon Public Utilities Commission has jurisdiction to investigate activities of Oregon telecommunications companies under ORS Chapter 756. None of the reasons cited by the FCC, or any of the state decisions referenced in Verizon's response, provide any basis for the Commission to reject the ACLU's request for an investigation. In fact, the Vermont Commissioner's comments are more instructive, recognizing that a state commission has a duty to protect the interests of its own citizens even when, or especially because, the federal government or other states will not.

D. The Telecommunications Companies' Statements of Nonparticipation Are Insufficient Bases for Concluding that the Companies Have Not Disclosed Customer Information in Violation of Oregon Law and Regulation.

The Commission should fully investigate whether the telecommunications companies improperly disclosed customer information to any person or entity, government or private, and not rely on vague or limited statements from the companies regarding possible disclosures. A full and thorough investigation will serve two important functions. First, it will uncover whether legally-protected personal information regarding Oregon citizens' intra-state communications has been improperly disclosed in any way. Second, a thorough investigation will clarify the legal and regulatory framework under which telecommunications companies can disclose certain customer information, thereby improving the future safety of

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

Oregon citizens' protected personal information.

United, in its response, states that, "to the best of its knowledge, it has not provided any customer information to the NSA." Response of United Telephone Company of the Northwest to ACLU Complaint, Public Utility Commission of Oregon, UM 1265 (July 5, 2006). This response is insufficient because it begs additional questions. As it noted in its Motion for Extension of Time to Respond, United was recently separated from SprintNextel Corporation. Motion of United for Extension of Time to Respond, Public Utilities Commission of Oregon, UM 1265 (June 12, 2006). United's response does not clarify whether it speaks to only the activities of United since its formation as a separate entity or those of both United and its predecessor companies. Further, United's response does not clarify whether United may have turned over customer information to any person or entity other than the NSA. The Commission should investigate whether United or any of its predecessor companies has disclosed any legally-protected customer information regarding Oregon intra-state communications to any person or entity, government or private, and if so under authority of what law. If United cannot attest to the activities of its predecessor companies, then the Commission should call upon SprintNextel Corporation to provide the necessary information.

Verizon, in its response, similarly states that "it has not turned over data on local calls to the NSA and in fact does not even make records of such calls in most cases." Response of Verizon Northwest, Public Utility Commission of Oregon, UM 1265 at 4 (July 5, 2005). Like United's response, Verizon's statement is too narrow to adequately address whether it has improperly disclosed any legally-protected customer information regarding Oregon intra-state communications to any third-party. And though it asserts that Verizon does not make records of local calls, the statement is too vague to determine what customer information is collected and

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

under what circumstances it has been or would be disclosed to any outside entities. Therefore, the Commission should seek clarification from Verizon and all Oregon telecommunications companies regarding the extent of the data they collect and the circumstances under which that data could be revealed to outside entities.

Because Qwest made no response to the ACLU's request for an investigation other than to acknowledge the request, the Commission should require Qwest to fully participate in any investigation the Commission initiates.

E. The Commission Should Conduct a Thorough Investigation into Oregon Telecommunications Companies' Handling of Legally-Protected Customer Information.

The replies of Qwest, United, and Verizon are insufficient to show that they have not revealed or would not reveal legally-protected customer information to outside entities. The Commission should conduct a thorough investigation in order to determine whether protected customer information and call contents are being safeguarded in full compliance with Oregon law. A full investigation should achieve the following:

(1) Determine what customer information the telecommunications companies collect about Oregon intra-state communications—whether local calls, toll calls, e-mail, or other communications.

(2) Determine in what situations, and under what authority, telecommunications companies have disclosed or would disclose that customer information to any other person or entity, government or private, including, but not limited to, service providers, marketing partners, law enforcement agencies, or other government entities.

(3) Determine whether any telecommunications companies have provided or would provide any third-party entity with access to its network, transmission systems, computer systems, software, or any other tools so that the third-party entity would have an ability to capture any legally-protected customer data without additional assistance by the companies.

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

(4) Determine all methods and tools—including both analog methods and tools and computer hardware and software—employed by telecommunications companies which are capable of tapping, listening to, recording, or otherwise accessing the content of intra-state voice and data communications.

(5) Determine the telecommunications companies' clear and detailed policies and practices regarding all circumstances under which they would employ any of the above methods or tools to tap, listen to, record, or otherwise access the content of intra-state voice or data communications, including to what extent these activities are required for the companies to operate in the normal course of business.

(6) Determine in what situations, and under what authority, telecommunications companies have allowed or would allow a third-party entity to obtain or access recordings, transcripts, printouts, or any other output resulting from the companies' tapping, listening to, recording, or other accessing of the content of intra-state voice or data communications.

(7) Determine in what situations, and under what authority, telecommunications companies have allowed or would allow a third-party entity to access its network, transmission systems, computer systems, software, or any other tools for the purpose of tapping, listening to, recording, or otherwise accessing the content of customer voice or data communications without additional assistance by the companies.

Regarding third-party access to either customer data or communication contents, the investigation should compel the companies to specifically discuss the circumstances and legal authority under which each would allow such access to (a) any local, state, federal, or foreign law enforcement entity; (b) any non-law-enforcement local, state, federal, or foreign government entity; and (c) any private, non-government third-party entity.

To the extent that its original request for an investigation may have indicated that any such investigation should be limited to the telecommunications companies' disclosure of customer data to the NSA, the ACLU hereby clarifies its request for an investigation to include the full inquiries into the disclosure of data or content from intra-state communications as described above.

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

F. Verizon's Procedural Objections Are Without Merit.

Verizon raises certain procedural objections that may best be characterized as form over substance. The ACLU clearly entitled its original submission a "Complaint and Request for Investigation." Its filing was in writing, contained the full name and address of each party complainant and each party defendant and set forth both sufficient facts and applicable rules and statutes so as to advise the parties and the Commission of the grounds of the complaint and the relief requested; that much is clear given Verizon's ability to respond with a 10 page document. As a consequence, the ACLU's filing satisfies the requirements of OAR 860-013-0015.

DATED this 20th day of July, 2006.

Respectfully submitted,

GARVEY SCHUBERT BARER

By _____

Keith S. Dubanevich, OSB #97520
E-Mail: kdubanevich@gsblaw.com
Mark E. Friedman, OSB #73094
E-Mail: mfriedman@gsblaw.com
Telephone: (503) 228-3939
Facsimile: (503) 226-0259

Attorneys for Complainant American Civil Liberties Union of Oregon

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 **AMERICAN CIVIL LIBERTIES UNION OF OREGON'S REPLY TO RESPONSES OF QWEST, UNITED TELEPHONE COMPANY OF THE NORTHWEST D/B/A EMBARQ, AND VERIZON NORTHWEST, INC.** 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

William E. Hendricks
Sprint/United Telephone Co. of the Northwest
902 Wasco Street, A0412
Hood River, OR 97031
E-Mail: tre.e.hendricks.iii@sprint.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., Suite 150
Hillsboro, OR 97006-4771
E-mail: renee.willer@verizon.com

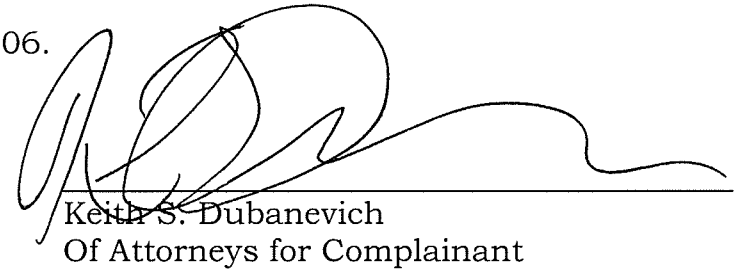
Citizens' Utility Board of Oregon
OPUC Dockets
610 SW Broadway, Ste. 308
Portland, OR 97205
E-Mail: dockets@oregoncub.org

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

/ / /

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

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 July 20, 2006.



Keith S. Dubanevich
Of Attorneys for Complainant

PDX_DOCS:376236.4 [30186-00114]

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

TITLE 18--CRIMES AND CRIMINAL PROCEDURE

PART I--CRIMES

CHAPTER 119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec. 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who--

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede,

or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

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

(A) a court order directing such assistance signed by the authorizing judge, or

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

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or

to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted--

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter--

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)(a)(i) If the communication is--

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection--

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

(Added Pub. L. 90-351, title III, Sec. 802, June 19, 1968, 82 Stat. 213; amended Pub. L. 91-358, title II, Sec. 211(a), July 29, 1970, 84 Stat. 654; Pub. L. 95-511, title II, Sec. 201(a)-(c), Oct. 25, 1978, 92 Stat. 1796, 1797; Pub. L. 98-549, Sec. 6(b)(2), Oct. 30, 1984, 98 Stat. 2804; Pub. L. 99-508, title I, Secs. 101(b), (c)(1), (5), (6), (d), (f)[(1)], 102, Oct. 21, 1986, 100 Stat. 1849, 1851-1853; Pub. L. 103-322, title XXXII, Sec. 320901, title XXXIII, Sec. 330016(1)(G), Sept. 13, 1994, 108 Stat. 2123, 2147; Pub. L. 103-414, title II, Secs. 202(b), 204, 205, Oct. 25, 1994, 108 Stat. 4290, 4291; Pub. L. 104-294, title VI, Sec. 604(b)(42), Oct. 11, 1996, 110 Stat. 3509; Pub. L. 107-56, title II, Secs. 204, 217(2), Oct. 26, 2001, 115 Stat. 281, 291; Pub. L. 107-296, title II, Sec. 225(h)(2), (j)(1), Nov. 25, 2002, 116 Stat. 2158.)

TITLE 18--CRIMES AND CRIMINAL PROCEDURE

PART I--CRIMES

CHAPTER 119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec. 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that

jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that--

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day

period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(a) an emergency situation exists that involves--

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any

wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)(a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of--

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved.

This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that--

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if--

(a) in the case of an application with respect to the interception of an oral communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or

electronic communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

(Added Pub. L. 90-351, title III, Sec. 802, June 19, 1968, 82 Stat. 218; amended Pub. L. 91-358, title II, Sec. 211(b), July 29, 1970, 84 Stat. 654; Pub. L. 95-511, title II, Sec. 201(d)-(g), Oct. 25, 1978, 92 Stat. 1797, 1798; Pub. L. 98-473, title II, Sec. 1203(a), (b), Oct. 12, 1984, 98 Stat. 2152; Pub. L. 99-508, title I, Secs. 101(c)(1)(A), (8), (e), 106(a)-(d)(3), Oct. 21, 1986, 100 Stat. 1851-1853, 1856, 1857; Pub. L. 103-414, title II, Sec. 201(b)(1), Oct. 25, 1994, 108 Stat. 4290; Pub. L. 105-272, title VI, Sec. 604, Oct. 20, 1998, 112 Stat. 2413.)

TITLE 18--CRIMES AND CRIMINAL PROCEDURE

PART I--CRIMES

CHAPTER 121--STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec. 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.--Except as provided in subsection (b)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.--A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

(B) if required by section 227 of the Crime Control Act of 1990; or

(7) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for Disclosure of Customer Records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

(5) to any person other than a governmental entity.

(Added Pub. L. 99-508, title II, Sec. 201[(a)], Oct. 21, 1986, 100 Stat. 1860; amended Pub. L. 100-690, title VII, Sec. 7037, Nov. 18, 1988, 102 Stat. 4399; Pub. L. 105-314, title VI, Sec. 604(b), Oct. 30, 1998, 112 Stat. 2984; Pub. L. 107-56, title II, Sec. 212(a)(1), Oct. 26, 2001, 115 Stat. 284; Pub. L. 107-296, title II, Sec. 225(d)(1), Nov. 25, 2002, 116 Stat. 2157.)

TITLE 18--CRIMES AND CRIMINAL PROCEDURE

PART I--CRIMES

CHAPTER 121--STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec. 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to Provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required Certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of Certain Disclosure.--No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by Bureau.--The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement That Certain Congressional Bodies Be Informed.--On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate,

concerning all requests made under subsection (b) of this section.

(Added Pub. L. 99-508, title II, Sec. 201[(a)], Oct. 21, 1986, 100 Stat. 1867; amended Pub. L. 103-142, Nov. 17, 1993, 107 Stat. 1491; Pub. L. 104-293, title VI, Sec. 601(a), Oct. 11, 1996, 110 Stat. 3469; Pub. L. 107-56, title V, Sec. 505(a), Oct. 26, 2001, 115 Stat. 365.)

TITLE 50--WAR AND NATIONAL DEFENSE

CHAPTER 36--FOREIGN INTELLIGENCE SURVEILLANCE

SUBCHAPTER I--ELECTRONIC SURVEILLANCE

Sec. 1805. Issuance of order

(a) Necessary findings

Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that--

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

(2) the application has been made by a Federal officer and approved by the Attorney General;

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that--

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under section 1804(h) of this title; and

(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

(b) Determination of probable cause

In determining whether or not probable cause exists for purposes of an order under subsection (a)(3) of this section, a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c) Specifications and directions of orders

An order approving an electronic surveillance under this section shall--

(1) specify--

(A) the identity, if known, or a description of the target of the electronic surveillance;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; and

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device; and

(2) direct--

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(d) Exclusion of certain information respecting foreign power targets

Whenever the target of the electronic surveillance is a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order need not contain the information required by subparagraphs (C), (D), and (F) of subsection (c)(1) of this section, but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.

(e) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated

(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, for the period specified in the application or for one year,

whichever is less, and (B) an order under this chapter for a surveillance targeted against an agent of a foreign power, as defined in section 1801(b)(1)(A) of this title may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this subchapter may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that (A) an extension of an order under this chapter for a surveillance targeted against a foreign power, as defined in section 1801(a)(5) or (6) of this title, or against a foreign power as defined in section 1801(a)(4) of this title that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this chapter for a surveillance targeted against an agent of a foreign power as defined in section 1801(b)(1)(A) of this title may be for a period not to exceed 1 year.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(f) Emergency orders

Notwithstanding any other provision of this subchapter, when the Attorney General reasonably determines that--

(1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and

(2) the factual basis for issuance of an order under this subchapter to approve such surveillance exists;

he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 1803 of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this subchapter is made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 72 hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any

United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title.

(g) Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel

Notwithstanding any other provision of this subchapter, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to--

(1) test the capability of electronic equipment, if--

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and:

(D) Provided, That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if--

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, or section 605 of title 47, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if--

(A) it is not reasonable to--

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this subchapter; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(h) Retention of certifications, applications and orders

Certifications made by the Attorney General pursuant to section 1802(a) of this title and applications made and orders granted under this subchapter shall be retained for a period of at least ten years from the date of the certification or application.

(i) Bar to legal action

No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this chapter for electronic surveillance or physical search.

(Pub. L. 95-511, title I, Sec. 105, Oct. 25, 1978, 92 Stat. 1790; Pub. L. 98-549, Sec. 6(b)(3), Oct. 30, 1984, 98 Stat. 2804; Pub. L. 106-567, title VI, Sec. 602(b), Dec. 27, 2000, 114 Stat. 2851; Pub. L. 107-56, title II, Secs. 206, 207(a)(1), (b)(1), 225, Oct. 26, 2001, 115 Stat. 282, 295; Pub. L. 107-108, title III, Sec. 314(a)(2), (c)(1), Dec. 28, 2001, 115 Stat. 1402, 1403.)

TITLE 50--WAR AND NATIONAL DEFENSE

CHAPTER 36--FOREIGN INTELLIGENCE SURVEILLANCE

SUBCHAPTER III--PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

Sec. 1843. Authorization during emergencies

(a) Requirements for authorization

Notwithstanding any other provision of this subchapter, when the Attorney General makes a determination described in subsection (b) of this section, the Attorney General may authorize the installation and use of a pen register or trap and trace device on an emergency basis to gather foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution if--

(1) a judge referred to in section 1842(b) of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to install and use the pen register or trap and trace device, as the case may be, on an emergency basis; and

(2) an application in accordance with section 1842 of this title is made to such judge as soon as practicable, but not more than 48 hours, after the Attorney General authorizes the installation and use of the pen register or trap and trace device, as the case may be, under this section.

(b) Determination of emergency and factual basis

A determination under this subsection is a reasonable determination by the Attorney General that--

(1) an emergency requires the installation and use of a pen register or trap and trace device to obtain foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title; and

(2) the factual basis for issuance of an order under such section 1842 of this title to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.

(c) Effect of absence of order

(1) In the absence of an order applied for under subsection (a)(2) of this section approving the installation and use of a pen register or trap and trace device authorized under this section, the installation and use of the pen register or trap and trace device, as the case may

be, shall terminate at the earlier of--

(A) when the information sought is obtained;

(B) when the application for the order is denied under section 1842 of this title; or

(C) 48 hours after the time of the authorization by the Attorney General.

(2) In the event that an application for an order applied for under subsection (a)(2) of this section is denied, or in any other case where the installation and use of a pen register or trap and trace device under this section is terminated and no order under section 1842 of this title is issued approving the installation and use of the pen register or trap and trace device, as the case may be, no information obtained or evidence derived from the use of the pen register or trap and trace device, as the case may be, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from the use of the pen register or trap and trace device, as the case may be, shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(Pub. L. 95-511, title IV, Sec. 403, as added Pub. L. 105-272, title VI, Sec. 601(2), Oct. 20, 1998, 112 Stat. 2407; amended Pub. L. 107-56, title II, Sec. 214(b), Oct. 26, 2001, 115 Stat. 287.)

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

ACLU of Oregon's Reply
Exhibit 2
Page 1 of 1

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

ACLU of Oregon's Reply
Exhibit 3
Page 1 of 1

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)

Rutland Herald
This is a printer friendly version of an article from www.rutlandherald.com
To print this article open the file menu and choose Print.

Back

Article published Jun 3, 2006

State orders inquiry into phone record flap

MONTPELIER — Vermont regulators have been called upon to investigate potentially illegal government access to records of phone company customers. According to state officials — including Gov. James Douglas — they have been dissatisfied with recent responses from phone companies on the matter.

Following news reports that AT&T and Verizon, which operate in Vermont, may have made records of domestic phone calls available to the federal National Security Agency, Vermont officials asked the firms in May for details about the matter.

The responses they recently received are symbolic of the "nonchalant" attitude the companies are taking in the matter, said Jason Gibbs, spokesman for Douglas.

"The response we received from them was thoroughly inappropriate from the administration's point of view," Gibbs said. "The governor has ordered the commissioner of public service to request that the Public Service Board open an investigation."

David O'Brien, commissioner of public service, said the state understands the need for security measures to protect against terrorism. However, Vermont customers have a right to know whether information about their phone use is not being kept private, and his department is charged with protecting those consumers and ensuring that any release of records is done properly.

It is sometimes the job of the states "to make sure the federal government, or these companies at the request of the federal government, don't cross certain lines," O'Brien said. "We don't want a government that doesn't trust anyone."

Vermont has little say over the NSA. However, it does have some control over utility companies such as Verizon and AT&T that do business here, O'Brien said.

There may be claims by the companies that federal authority preempts the states.

"That is, in part, what we are trying to sort out," he said.

Officials of the two companies declined to comment beyond statements made in response to O'Brien's requests.

AT&T's response is two paragraphs long, stating in part, "if and when AT&T is asked by a government agency for assistance, we do so strictly within the law. Beyond that AT&T cannot comment on matters of national security. Questions regarding such matters must be addressed on a national basis."

Verizon's several-page response is more comprehensive and appears to be an attempt to legitimately answer the request for information, O'Brien said. However, it still does not adequately answer the concerns raised, he said.

The company reiterated that it has not turned over records of calls and does not make records of such calls in most cases.

But the company stated, "Verizon is prohibited from providing any information concerning its alleged cooperation with the NSA program," according to the company's letter. "It is a felony under federal criminal law for any person to divulge classified information," the letter stated.

Although the company acknowledges cooperating when required to do so by law enforcement officials, any information relating to whether it was or was not part of the alleged NSA program is protected by national secrecy regulations.

Verizon's response is "like a page out of George Orwell," said Allen Gilbert, executive director of the Vermont American Civil Liberties Union. "It seems that, in the end, the document just creates more suspicion. More suspicion of the government and more suspicion of the companies."

What good is a company's privacy policy if it cannot be relied on, Gilbert said.

O'Brien said he understands the companies are in some ways caught between the federal government and the state government. However, Vermont consumers have to be assured that if their phone records are accessed by government officials it is done through legal means.

"We need to know more," he said. "Give us some comfort ... this was done in the right way."

Verizon made a related argument in Maine, where that state's Public Utilities Commission is considering a similar complaint against the company.

Verizon said that case, brought by 12 Mainers, should be dismissed because the matter is "highly classified," according to news reports. As in the Vermont case,

Verizon said it could neither confirm nor deny its participation in the NSA program because of secrecy rules.

Meanwhile the states appear unlikely to get much cooperation from the federal government in the matter.

For instance, a California lawsuit over the issue should be dismissed for security reasons, testified John Negroponte, the director of national intelligence, who is expected to speak at Monday's St. Johnsbury Academy graduation.

On May 12, Negroponte asserted "the military and state secrets privilege" in a declaration to the U.S. District Court, saying that "further litigation will risk the disclosure of information harmful to the national security of the United States and, accordingly, this case should be dismissed."

Gibbs said the state will continue to seek a satisfactory response from the companies. "They essentially, using a bunch of legal mumbo jumbo, told Vermont's consumers, whose phone records may have been illegally released, to go pound sand, and the governor's just not going to tolerate that."

Contact Louis Porter at louis.porter@timesargus.com louis.
porter@rutlandherald.com.
