June 30, 2006

Washington Utilities and Transportation Commission
P.O. Box 47250
1300 S. Evergreen Park Dr. SW
Olympia, WA 98504-7250

Docket #UT-060856
Comments by American Civil Liberties Union of Washington

Dear Chairman Sidran and Commission Members:

AMERICAN CIVIL
LIBERTIES UNION OF
WASHINGTON
FOUNDATION
705 2ND AVENUE, 3RD FL.
SEATTLE, WA 98104
T/206.624.2184
F/206.624.2190
WWW.ACLU-WA.ORG

TIMOTHY KAUFMAN-OSBORN
BOARD PRESIDENT

KATHLEEN TAYLOR
EXECUTIVE DIRECTOR

The American Civil Liberties Union of Washington (ACLU-WA) welcomes this opportunity to comment on threshold issues relevant to your possible investigation of improper disclosure of telephone records.

**Statement of Interest**

The ACLU-WA is an organization of over 25,000 members in Washington, dedicated to defending civil liberties, including the right to personal information privacy. For more than two decades, we have advocated in judicial, regulatory, and legislative arenas for the protection of telephone records in order to preserve the privacy of telephone users. These records contain sensitive information about people, potentially revealing their associations, interests and a host of personal details about their lives.

Most recently, we have been concerned about public allegations that some telephone companies have engaged in wholesale disclosure of telephone calling records without legal authorization. We accordingly asked the Utilities and Transportation Commission to investigate the practices of telecommunications companies doing business within Washington, to determine whether any telephone records of Washington consumers have been improperly disclosed. We appreciate the Commission's willingness to consider such an investigation, and now offer the following comments on the specific questions asked by the Commission.

**Does WAC 480-120-202 or any other state law or regulation prohibit a regulated telephone company or its affiliated interests from providing customer telephone calling information to the National Security Agency (NSA)?**

The quick answer to this question is "yes," in the absence of a warrant or other legal process, as discussed below. However, the initial question should be worded more broadly, to ask whether disclosure of customer telephone calling information to any third party without customer consent or legal process is a violation of law. The Commission need not determine to whom calling information has been disclosed, nor learn anything about the subsequent use of that information—it is the disclosure itself, to any entity, that violates law.

Further, the Commission should not limit the question to only state law and regulations; its jurisdiction extends to all telecommunication company acts done "in violation, or claimed to be in violation, of any provision of law." RCW 80.04.110(1). Nothing in the statute implies this jurisdiction is limited to investigation of violations of *state* law alone. Nor should it; as the organization within the state most familiar with telecommunication companies, it is logical that the Commission be charged with investigation of potentially illegal practices by those companies, no matter what the source of applicable law.

WAC 480-120-202 is the state law regulating disclosure of telephone calling records, a form of "customer proprietary network information" (CPNI).[1] It "adopts by reference the Federal Communications Commission's rules" for use and disclosure of CPNI by "all telecommunications carriers providing wireline, intrastate telecommunications service in Washington." WAC 480-120-202.

In turn, 47 C.F.R. § 64.2005 (the applicable FCC rule) specifies the limited circumstances in which CPNI may be disclosed without customer approval. Disclosure is permitted for some marketing activities, the provision of some information services (such as voice mail), the "provision of inside wiring installation, maintenance, and repair services," research on health effects of wireless services, and "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." All other disclosures of CPNI, unless *required* by a separate law, are unlawful without the approval of the customer.[2]

---

[1] CPNI is defined as:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
>
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; information the phone company obtains when it provides phone service including the types of services purchased, the usage of those services, and the related billing of those services.

47 U.S.C. § 222(h)(1). Call detail records, or any other records of telephone numbers called by subscribers, fall within the definition of CPNI.

[2] Although the rule itself primarily discusses the circumstances under which CPNI *may* be disclosed, it must be read in conjunction with its authorizing statute, which generally prohibits disclosure of CPNI

The FCC rules further define what qualifies as customer approval. For all purposes other than marketing, "a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval." 47 C.F.R. § 64.2007(b)(3). Opt-in approval requires "affirmative, express consent" after "appropriate notification" of the intended disclosure. 47 C.F.R. § 64.2003(h).

In summary, it is a violation of WAC 480-120-202 to disclose telephone calling information to any person or entity without the express consent of the telephone customer, except for limited purposes related to provision or marketing of telephone services.

Disclosure of telephone records under such circumstances is also a violation of Federal statutes. 47 U.S.C. § 222 essentially mirrors Washington's regulation of disclosure of CPNI. In addition, a provider of telephone service "shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service ... to any governmental entity." 18 U.S.C. § 2702(a)(3). Naturally, there are several statutory exceptions to this prohibition, largely along the same lines as permitted disclosures of CPNI. Disclosure is allowed pursuant to legal process, 18 U.S.C. § 2703(c), "incident to the rendition of service" or to protect the company's property, 18 U.S.C. § 2702(c)(3), or pursuant to customer consent, 18 U.S.C. § 2702(c)(2); 18 U.S.C. § 2703(c)(1)(C). Although not further defined, it is reasonable to believe that, as with CPNI, this requires explicit affirmative assent by the customer. The only additional exception is that disclosure of records may be allowed in an emergency, 18 U.S.C. § 2702(c)(4); the exact parameters of this section have changed with recent legislation, but both new and old versions require an emergency threatening death or serious physical injury, and are limited to threats to specific individuals.

Hence, bulk disclosure of telephone records to a governmental entity with neither legal process nor explicit customer consent is a violation of federal law.

Federal law limits the Commission's adjudicatory jurisdiction over violations of the Federal CPNI statute. 47 U.S.C. § 207. This does not affect the Commission's authority to investigate violations of state CPNI law, nor is there a similar stripping of jurisdiction with regard to violations of 18 U.S.C. § 2702. Even if the Commission somehow is determined not to have jurisdiction to adjudicate these violations, an investigation is still warranted. The Commission may "initiate and/or participate in proceedings before federal administrative agencies in which there is at issue the authority, rates or *practices* for transportation or utility services ... and [may] similarly initiate and/or participate in any judicial proceedings

---

"[e]xcept as required by law or with the approval of the customer," or as necessary to provide telecommunications services. 47 U.S.C. § 222(c)(1). Thus, any disclosure that does not fall within those permitted by 47 C.F.R. § 64.2005 is prohibited.

relating thereto." RCW 80.01.075 (emphasis added). In so doing, the Commission has full investigative powers, as it may "do all things necessary in its opinion to present to such federal administrative agencies all facts bearing upon such issues." *Id.* Thus, whether or not the Commission has jurisdiction to adjudicate complaints regarding potential violations of federal law by telecommunications companies, it is clearly empowered to investigate such practices.

**Does the Commission have the legal authority to compel a regulated telephone company or its affiliates to disclose whether it has provided customer calling information to the NSA?**

The Commission clearly has the authority to investigate unlawful practices of telephone companies, including improper disclosures of customer information. Even minimally regulated competitive companies are required to "[c]ooperate with commission investigations of customer complaints." RCW 80.36.320(2)(d). At a minimum, that would seem to require a simple statement from every company as to whether or not it has disclosed bulk customer records outside of the company. If companies choose not to honor their duty to cooperate, the Commission can compel cooperation through its power to issue subpoenas, and the ability to audit books and records of companies. If a preliminary investigation provides basis for a formal complaint, the entire range of discovery options will also be available.

The only substantial question about the Commission's authority is whether its general investigative powers are limited because allegations of telecommunications company wrongdoing have also implicated the NSA. There is a colorable argument that Section 6 of the National Security Act of 1959 preempts the Commission's authority to compel disclosure of information regarding the NSA or its functions. However, assertion of such a claim requires a specific showing that information about the NSA will be revealed that is not already well publicized. *See Founding Church of Scientology v. NSA*, 610 F.2d 824 (D.C. Cir. 1979). And there is an argument under the separations of powers doctrine that Congress does not have the power to eliminate judicial and quasi-judicial investigations, so the Act should be interpreted not to apply to such investigations.

The Commission need not resolve this thorny legal issue, however. As with the Commission's first question, the ACLU-WA would suggest a reframing of the question to instead ask simply whether the Commission has the authority to compel a telephone company to disclose whether or not it has released customer calling information outside the company. As before, it is irrelevant who the recipient of the calling information may have been—and the National Security Act is not implicated.

To determine whether WAC 480-120-202 has been violated, only three facts need to be determined. First, has the company disclosed CPNI to a third party?

Second, if so, how were customers notified in advance of the proposed disclosure? Third, how was consent obtained from the customers for the disclosure, and how was CPNI segregated for those that did not consent?

Similarly, to determine whether 18 U.S.C. § 2702 was violated, only a few questions need be answered. First, were telephone records disclosed to a governmental entity? Second, if so, what was the authorization for disclosure? Did customers consent to the disclosure; if so, how was the consent obtained? If customers did not consent, what legal document (e.g., warrant, court order, or subpoena) was provided to the company to authorize disclosure?

Some telephone companies have implied that they will be unable to answer requests for information from the Commission because they would be required to disclose classified information. *See* AT&T Response to ACLU Letter (May 26, 2006). With the narrowed scope of the question we suggest, such a claim is not viable.

None of the limited information necessary to answer the above questions should be classified, as it is not "owned by, produced by or for, or ... under the control of the United States Government." Exec. Order No. 13,292 § 1.1(2) (2003). Nor does it fall within the limited categories of information eligible for classification, Exec. Order No. 13,292 § 1.4, since that is all information related to government operations, not the records maintenance practices of private companies. Similarly, a telephone company's claim that it is unable to confirm or deny record sharing due to revelation of classified information is simply untenable. In contrast to AT&T, the Washington Independent Telephone Association has denied that any of its members have disclosed telephone records to government agencies except with specific subpoenas or warrants. *See* WITA Letter (June 8, 2006). Why would other telecommunications companies be unable to do the same?

Despite claims to the contrary, telecommunications companies can disclose the legal authorization requiring them to disclose customer information. A similar question was addressed in *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005). In that case, the plaintiff, a Connecticut library, received a National Security Letter (NSL) requiring it to disclose patron information, and prohibiting it from disclosing the receipt of the NSL. The library challenged the non-disclosure provision, and the court granted a preliminary injunction, finding that "plaintiffs have shown a substantial likelihood of success on the merits." *Id.* at 82. The court found that the government did not have a compelling interest in concealing the library's identity as a recipient of an NSL. *Id.* at 78. Although the precise holding was limited to a particular NSL given to a particular library, the logic applies equally well to any form of legal authorization given to a telephone company. Disclosure of that general information cannot serve to harm national security investigations. The claimed need for secrecy is particularly unsupported when, as here, the general information has already been widely publicized.

**Does the Commission have the legal authority to compel regulated telephone companies or their affiliates to release relevant information about such allegations?**

This is a more difficult question to answer, as we do not know what is contained in documents held by telephone companies. If companies did, in fact, share records with the National Security Agency or another intelligence agency, it is quite possible that some documents discussing some aspects of the sharing may be classified—and thus cannot be disclosed to the Commission unless Commission members have the appropriate security clearances.

It is equally likely, however, that other documents discussing either disclosure of customer records, or legal authority to do so, are not classified. That is especially likely for documents found in companies, such as Qwest, that reportedly denied requests to share information. And, of course, any disclosure of records to either non-intelligence or non-governmental entities should not involve any classified information whatsoever.

If telephone records have been released without legal authorization, that is a violation of law. Our nation's system of information classification must not be used to "conceal violations of law, inefficiency, or administrative error." Exec. Order No. 13292 § 1.7(a)(1). The same principle would indicate that claims of potentially classified information should not be used to deter an investigation of wrongdoing—instead, the investigation should be allowed to move forward until, and unless, it reaches a point where the only further relevant information is classified, and no security clearance is possible to examine that information.

Such a point is unlikely to arise with this investigation. As discussed above, all of the key relevant information has to do with the telephone companies' own practices, and should not be classified. Certainly the basic facts of whether disclosure has occurred, and under what authority, should be available to the Commission, and those facts are sufficient to determine whether the law has been violated.

**Would an assertion of the military and state secrets privilege by the United States Government preclude the Commission from taking action against a regulated telecommunications company?**

The first fact that must be emphasized is that no interested party has thus far asserted the state secrets privilege to this Commission. The privilege "belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party." *United States v. Reynolds*, 345 U.S. 1, 8 (1953). It is simply speculation that the United States Government will assert the privilege, since such an assertion is not undertaken lightly. The privilege may only be asserted by "by the head of the department which has control over the matter, after actual

personal consideration by that officer." *Id.* Assuming the Commission investigation is structured to have limited scope, as suggested above, no state secrets will be at risk from the investigation; in such a case, there will be no reason for a department head to take the weighty step of asserting the privilege.

Some guidance may be found from proceedings currently underway in New Jersey. There, the state Attorney General issued subpoenas to several telephone companies shortly after USA Today published its initial story. Two weeks ago, the United States filed a complaint in federal court, asking for the subpoenas to be quashed. *See* United States Complaint (June 14, 2006). Significantly, although the state secrets privilege was discussed in the complaint, the United States did *not* assert the privilege. Perhaps it will yet do so, but that should not be assumed—nor should it be assumed that the privilege will be invoked here.

Assuming the privilege is asserted, that still need not end a Commission investigation. The mere invocation of the privilege does not determine its applicability. "Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers." *Reynolds*, 345 U.S. at 9. The tribunal must make an independent examination of the claim, and must be satisfied "from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged." *Id.* at 10.

The United States has asserted the state secrets privilege in one lawsuit regarding telecommunications company cooperation with warrantless interception of communications by the NSA, *Hepting v. AT&T Corp., et. al*, Case No. C-06-0672-VRW (N.D. Cal.). That court has yet to rule whether the privilege is applicable. Even if does eventually determine the privilege applies, such determination does not automatically extend to a Commission investigation of an entirely separate issue, the practices of telecommunications companies in disclosure of customer records.

Ultimately, the state secrets privilege is simply an evidentiary privilege,[3] and serves only to protect certain information from disclosure. Only in the most extreme cases, where information at the core of the proceeding involves state secrets, may entire complaints be dismissed; this "is a drastic remedy that has rarely been invoked." *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1242 (4th Cir. 1985) (citing numerous cases in which proceedings continued after the claim of state secrets privilege prevailed). The normal procedure is to continue without the privileged evidence—the same process used for every other privilege.

[3] As an evidentiary privilege, it must be recognized in the jurisdiction in which the privilege is asserted. As far as the ACLU-WA knows, no Washington court has ever had occasion to consider whether or not the state secrets privilege applies in Washington state fora.

In the present situation, there is no reason to believe that an investigation cannot continue even if the United States prevails in a claim of the state secrets privilege to keep some information away from the Commission. As discussed above, only a very few facts need be discovered, and these facts are related only to the companies' own practices, and do not implicate state secrets at all. Invocation of the privilege to protect some tangential material will thus not keep the Commission from examining the information central to its investigation.

**If the Commission decides to investigate the matter raised in the ACLU's May 25, 2006, letter, which procedural options would be most appropriate? (e.g., informal investigation, formal investigation, complaint).**

The ACLU-WA defers to the Commission's expertise in fashioning the most appropriate form of investigation. We are concerned only that a true investigation take place in order to discover the facts related to disclosure of telephone records. At this point, there is not enough information to know whether any violation of law has occurred, or to suggest the most effective steps the Commission can take to prevent future violations.

The present factual uncertainty suggests that an informal investigation may be the best first step. If telecommunications companies take seriously their duty to cooperate with the Commission's investigation, quite a bit of information can be determined in the course of an informal investigation. As an example, just the discussion of the possibility of an investigation has already caused some telephone companies to explain their record disclosure process and to confirm that they have not provided wholesale customer information to government agencies. *See* WITA Letter (June 8, 2006). The ACLU-WA hopes that a Commission investigation, whether informal or formal, will obtain the same information from other companies providing telecommunications services within Washington State.

Sincerely,

Doug Klunder
Privacy Project Director