

**BEFORE THE WASHINGTON UTILITIES AND  
TRANSPORTATION COMMISSION**

In the Matter of Adopting and Repealing:	)	
	)	DOCKET NO. UT-990146
	)	
WAC 480-120-201 through WAC 480-120-209 and WAC 480-120-211 through WAC 480-120-216	)	GENERAL ORDER NO. R-505
	)	
Relating to Telecommunications Companies - Customer Information Rules.	)	ORDER ADOPTING AND REPEALING RULES PERMANENTLY
.....	)	

*1* **SYNOPSIS:** *The Commission adopts rules governing how telecommunications companies may use information they possess about the telecommunications services a particular customer uses and how the customer uses them. The rules follow the framework of corresponding rules recently adopted by the Federal Communications Commission, but contain three important differences:*

- The rules provide increased protection for particularly sensitive personal information, including the phone numbers a customer calls and including highly specific phone calling habits of the customer. A company may not use this information, known as “call detail,” without the customer’s express (“opt-in”) approval, except as necessary for the company to provide service or as required by law.*
- We narrow the scope of a telecommunications company’s “family” of affiliated companies, within which it may share information about a customer if the customer does not “opt-out.” The effect is to require express (“opt-in”) approval for disclosure to more types of entities than the federal rules require.*
- We improve the notice that companies must provide to customers, in order to help customers understand what is at stake. Also, by requiring companies to offer their customers more convenient methods for opting-out, we enhance customers’ ability to exercise that choice, where applicable.*

*In reaching these conclusions, the Commission balances protected rights of telecommunications companies to engage in commercial free speech, with customers’ rights to privacy and free speech and association, as reflected in our state and federal laws and constitutions. We have adopted rules that we think appropriately balance these interests under the law.*

2     **STATUTORY OR OTHER AUTHORITY:** The Washington Utilities and  
Transportation Commission takes this action under Notice WSR # 02-08-081,  
filed with the Code Reviser on April 3, 2002. The Commission brings this  
proceeding pursuant to RCW 80.01.040 and RCW 80.04.160.

3     **STATEMENT OF COMPLIANCE:** This proceeding complies with the  
Open Public Meetings Act (chapter 42.30 RCW), the Administrative Procedure  
Act (chapter 34.05 RCW), the State Register Act (chapter 34.08 RCW), the  
State Environmental Policy Act of 1971 (chapter 43.21C RCW), and the  
Regulatory Fairness Act (chapter 19.85 RCW).

4     **DATE OF ADOPTION:** The Commission adopts these rules on the date  
that this Order is entered.

5     **CONCISE STATEMENT OF PURPOSE AND EFFECT OF THE  
RULE:** RCW 34.05.325 requires that the Commission prepare and provide to  
commenters a concise explanatory statement about an adopted rule. The  
statement must include the identification of the reasons for adopting the rule, a  
summary of the comments received regarding the proposed rule, and responses  
reflecting the Commission's consideration of the comments. The Commission  
often includes a discussion of these matters in its rule adoption orders.

6     In this rulemaking, in order to avoid unnecessary duplication, the Commission  
designates the discussion in this order, including its attachments (appendices A  
and B), as its concise explanatory statement.

7     **REFERENCE TO AFFECTED RULES:** This order repeals the following  
sections of the Washington Administrative Code:

WAC 480-120-144	Use of privacy listings for telephone solicitation.
WAC 480-120-151	Telecommunications carriers' use of customer proprietary network information (CPNI).

WAC 480-120-152	Notice and approval required for use of customer proprietary network information (CPNI).
WAC 480-120-153	Safeguards required for use of customer proprietary network information (CPNI).
WAC 480-120-154	Definitions.

8 This Order adopts the following sections of the Washington Administrative Code:

WAC 480-120-201	Definitions.
WAC 480-120-203	Use of customer proprietary network information (CPNI) not permitted to identify or track customer calls to competing service providers.
WAC 480-120-204	Opt-in approval required for use, disclosure, or access to customer ICPNI.
WAC 480-120-205	Using customer proprietary network information (CPNI) in the provision of services.
WAC 480-120-206	Using individual customer proprietary network information (CPNI) during inbound and outbound telemarketing calls.
WAC 480-120-207	Use of private account information (PAI) by company or associated companies requires opt-out approval.
WAC 480-120-208	Use of customers' private account information (PAI) to market company products and services without customer approval.
WAC 480-120-209	Notice when use of private account information (PAI) is permitted unless a customer directs otherwise ("opt-out").
WAC 480-120-211	Mechanisms for opting out of use of private customer account information (PAI).
WAC 480-120-212	Notice when express ("opt-in") approval is required and mechanisms for express approval.

WAC 480-120-213	Confirming changes in customer approval status.
WAC 480-120-214	Duration of customer approval or disapproval
WAC 480-120-215	Safeguards required for CPNI.
WAC 480-120-216	Disclosing CPNI on request of customer.
WAC 480-120-217	Using privacy listings for telephone solicitation.
WAC 480-120-218	Using subscriber list information for purposes other than directory publishing.
WAC 480-120-219	Severability.

9 This Order withdraws the following proposed section of the Washington Administrative Code:

WAC 480-120-202	Use of customer proprietary network information (CPNI) permitted.
-----------------	---

10 **PREPROPOSAL STATEMENT OF INQUIRY AND ACTIONS THEREUNDER:** The Commission filed a Preproposal Statement of Inquiry (CR-101) on April 15, 1999, at WSR # 99-09-027.

11 **ADDITIONAL NOTICE AND ACTIVITY PURSUANT TO PREPROPOSAL STATEMENT:** The statement advised interested persons that the Commission was considering a rulemaking to review rules relating to regulated telephone companies for content and readability pursuant to Executive Order 97-02, with attention to the rules' need, effectiveness and efficiency, clarity, intent, and statutory authority, coordination, cost, and fairness. The statement also advised that the review would include consideration of whether substantive changes or additional rules are required for telecommunications regulation generally, in concert with the Federal Telecommunications Act of 1996 and potential actions by the Washington Legislature during its 1999 session. The Commission also provided notice of the subject and the CR-101 to all persons on the Commission's list of persons requesting such information pursuant to RCW 34.05.320(3), and sent notice to all registered telecommunications companies and to the Commission's list of telecommunications attorneys. The Commission posted the relevant rulemaking information on its internet web site at [www.wutc.wa.gov](http://www.wutc.wa.gov).

- 12 **MEETINGS AND WORKSHOPS; ORAL COMMENTS:** The Commission held several rulemaking workshops on draft rules in Docket No. UT-990146 concerning Chapter 480-120 WAC. At a workshop held on June 5, 6, and 7, 2001, WAC 480-120-144, "Use of privacy listings for telephone solicitation," was included on the agenda. That rule has been amended and adopted as WAC 480-120-217.
- 13 On January 23 and 24, 2002, the Commission held evening public meetings on the topic of privacy of customer telephone records. The meeting on January 23 was held in Bothell, Washington, and the January 24 meeting was held in Fife, Washington. The times and locations of the meetings were widely reported in the press in advance, both meetings were attended by members of the public, and both were reported on by the media.
- 14 The Commission held a special open meeting on February 5, 2002, for the purpose of considering adoption of an emergency rule on the topic of customer privacy. At the beginning of the meeting, the Commission informed attendees that it would not be taking action on an emergency rule, but invited participation in a discussion of the topic. Representatives of several large telecommunications companies spoke on the topic.
- 15 On March 14 and March 22, 2002, the Commission held half-day rulemaking workshops on issues related to customer privacy rules. These workshops were attended by representatives of a diverse interests, including telecommunications companies, public interest organizations, state agencies, and Public Counsel.
- 16 **NOTICE OF PROPOSED RULEMAKING:** The Commission filed a notice of Proposed Rulemaking (CR-102) on April 3, 2002, at WSR #02-08-081. The Commission scheduled this matter for oral comment and adoption under Notice WSR #02-08-081 at 9:30 a.m., Friday, July 26, 2002, in the Commission's Hearing Room, Second Floor, Chandler Plaza Building, 1300 S. Evergreen Park Drive S.W., Olympia, Washington. The Notice provided interested persons the opportunity to submit written comments to the Commission.
- 17 **COMMENTERS (WRITTEN COMMENTS):** The Commission received written comments from AARP, AT&T, Allegiance Telecom, Claudia Berry,

Elizabeth Clawson, Rep. Mary Lou Dickerson, Electronic Privacy Information Center (EPIC), Elizabeth Fehrenbach, Emeri Hansen, Gail Love, Low Income Telecommunications Project (LITE), Lindsay Olsen, Public Counsel Section of the Office of the Attorney General, Qwest, Senior Services, Sprint, Robert Stein, Matilda Stubbs, Destinee Sutton, Ben Unger, Verizon, WashPIRG, Washington Independent Telephone Association (WITA), and WorldCom.

18 **RULEMAKING HEARING:** The Commission originally scheduled this matter for oral comment and adoption under notice #02-08-081, at a rulemaking hearing scheduled during the Commission's regularly scheduled open public meeting on July 26, 2002, at the Commission's offices in Olympia, Washington. The Commission continued the rule adoption on the record of the July 26 hearing and by written notice to stakeholders who had participated in earlier phases of the rulemaking proceeding until August 20, 2002. On August 20, 2002, Chairwoman Marilyn Showalter, Commissioner Richard Hemstad, and Commissioner Patrick J. Oshie considered the rule proposal for adoption. The Commission heard oral comments from Qwest, Public Counsel Section of the Office of the Attorney General, Qwest, Seattle Telecommunications Consortium, Spokane Neighborhoods Action Program, Sprint, Verizon, WashPIRG, and WorldCom.

19 **COMMISSION ACTION:** After considering all of the information regarding this proposal, the Commission repealed and adopted the rules in the CR-102 at WSR #02-08-081 with the changes described in Appendix B.

20 **STATEMENT OF ACTION; STATEMENT OF EFFECTIVE DATE:** In reviewing the entire record, the Commission determines that WAC sections 480-120-144, 480-120-151, 480-120-152, 480-120-153, 480-120-154 should be repealed.

21 The Commission determines that WAC sections 480-120-201, 480-120-203, 480-120-204, 480-120-205, 480-120-206, 480-120-207, 480-120-208, 480-120-209, 480-120-211, 480-120-212, 480-120-213, 480-120-214, 480-120-215, 480-120-216 should be adopted to read as set forth in Appendix C, as rules of the Washington Utilities and Transportation Commission, to take effect pursuant to RCW 34.05.380(2) on January 1, 2003.

## COMMISSION ORDER

### I. BACKGROUND

#### A. Prior WUTC Rules Addressing Telecommunications Company Use of Non-Public Personal Information

22 This Commission adopted its first rule to protect the privacy of customer proprietary network information (CPNI)<sup>1</sup> in 1997.<sup>2</sup> That rule prohibited the use of CPNI for marketing purposes. In early 1999, we replaced that rule with rules<sup>3</sup> substantively identical to those adopted by the Federal Communications Commission (FCC) in 1998.<sup>4</sup> The FCC rules implemented § 222 (“Section 222”)<sup>5</sup> of the Federal Telecommunications Act of 1996 (the “1996 Act”). The FCC rules required carriers to obtain a customer’s express approval (or “opt-in”) before using or disclosing CPNI identifiable with that customer, for any purpose other than marketing additional communications services within the category of services to which the customer already subscribed. The “categories of service” defined by the rule were local, interexchange, and wireless.

---

<sup>1</sup> Under 47 U.S.C § 222, customer proprietary network information means: “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 information contained in the bills of pertaining to telephone exchange service or telephone toll service received by a customer of a carrier . . .”

<sup>2</sup> 97-18-056 Wash. St. Reg., § 480-120-139(5) (General Order No. R-442, Docket No. UT-960942) filed August 27, 1997.

<sup>3</sup> 99-05-015 Wash. St. Reg., § 480-120-151 et seq. (General Order No. R-459, Docket No. UT-971514) filed February 25, 1999.

<sup>4</sup> *In the Matter of Implementation of Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1988).

<sup>5</sup> Section 222(c)(1) of the 1996 Act provides: “PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS.—Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.”

## B. 10<sup>th</sup> Circuit Vacation of 1998 FCC Rules

- 23 The 10<sup>th</sup> Circuit U.S. Court of Appeals in *U.S. West v. F.C.C.*, 182 F.3d 1224 (10<sup>th</sup> Cir. 1999) vacated the portion of the FCC's CPNI rules that required customer opt-in, as an unjustified restriction on carriers' First Amendment commercial speech rights. The 10<sup>th</sup> circuit said that the FCC had failed to show that an alternative less restrictive of carriers' free speech rights, such as opt-out, would not sufficiently protect customer privacy. The U.S. Supreme Court declined to review the 10<sup>th</sup> Circuit decision.<sup>6</sup>
- 24 In response to the 10<sup>th</sup> Circuit decision, the FCC, in August 2001, issued an order reinterpreting its rules as requiring that customers need only be afforded the ability to "opt-out" of carriers' "use, disclosure or permission of access" to CPNI.<sup>7</sup> At the same time, the FCC initiated a new rulemaking on the topic of CPNI.
- 25 After the FCC's decision to reinterpret its rule in response to the 10<sup>th</sup> Circuit's *U.S. West* decision, Verizon asked the WUTC either to eliminate our state rules or to conform them to the new FCC interpretation. We first considered adopting substantive changes to our CPNI rules as a result of Verizon's request.
- 26 Following Verizon's request, Qwest mailed an opt-out notice to its customers that touched off alarm and angry reaction among consumers, consumer and privacy rights advocates, and the media. Based on intensely negative public response to its notice and its limited ability to accommodate customer requests to retain their privacy, Qwest retracted its notice. The Qwest experience served to highlight for the Commission the shortcomings of the implied consent or opt-out method of obtaining customer approval with respect to certain uses and certain types of CPNI.

---

<sup>6</sup> *Petition for cert. denied, Competition Policy Institute v. US WEST, Inc.*, 530 U.S. 1213 (June 2000).

<sup>7</sup> *In the Matter of Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115, 96-149, and 00-257, *Clarification Order and Second Further Notice of Proposed Rulemaking*, 16 FCC Rcd 16506 (August 28, 2001).



### C. New FCC Rule

27 In July of this year, the FCC adopted a new set of rules interpreting the requirements of § 222 of the Federal Telecommunications Act (Section 222), the statute on which the FCC's rules are based.<sup>8</sup> In its adoption order, the FCC expressly left the door open to more stringent state protection for CPNI.<sup>9</sup> It also stated, however, that it would be willing to preempt state rules that needlessly depart from national standards. Under the FCC's rules, *47 CFR Part 64*:

- Use of CPNI that is not identified with an individual is not restricted by the rules.
- Without providing any notice to the customer or securing the customer's permission to do so, carriers may use a customer's individually identifiable CPNI to market telecommunications services within the category of service which the carrier already provides to that customer.

---

<sup>8</sup>*In the Matter of Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers, Third Report and Order and Third Further Notice of Proposed Rulemaking (Released: July 25, 2002).*

<sup>9</sup>*Id.* at ¶¶ 69-74. The FCC stated:

“We conclude that carriers can use opt-out for their own marketing of communications-related services, as described above, which is less burdensome than opt-in. We reach this conclusion based on the record before us, but must acknowledge that states may develop different records should they choose to examine the use of CPNI for intrastate services. They may find further evidence of harm, or less evidence of burden on protected speech interests. Accordingly, applying the same standards, they may nevertheless find that more stringent approval requirements survive constitutional scrutiny, and thus adopt requirements that ‘go beyond those adopted by the Commission.’ While the Commission might still decide that such requirements could be preempted, it would not be appropriate for us to apply an automatic presumption that they will be preempted. We do not take lightly the potential impact that varying state regulations could have on carriers' ability to operate on a multi-state or nationwide basis. Nevertheless, our state counterparts do bring particular expertise to the table regarding competitive conditions and consumer protection issues in their jurisdictions, and privacy regulation, as part of general consumer protection, is not a uniquely federal matter. We decline, therefore, to apply any presumption that we will necessarily preempt more restrictive requirements.

\* \* \*

We note that we would be willing to preempt state requirements in the event that numerous different approval schemes make it impracticable for carriers to obtain customer approval for the use of CPNI. Carriers can always establish that burdens from state and federal CPNI regulation are unworkable. By reviewing requests for preemption on a case-by-case basis, we will be able to make preemption decisions based on the factual circumstances as they exist at the time on a full and complete record.”

The categories of service are local, interexchange, and wireless. Included within the local service category, in addition to basic local service, are services such as speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.

- Only after providing the customer with notice and an opportunity to opt-out may carriers use a customer's individually identifiable CPNI to market communications-related services outside of the category to which the customer already subscribes. The carrier may also disclose the customer's individually identifiable CPNI to its affiliates, agents, independent contractors and joint venture partners for the purpose of marketing communications-related services subject to the customer's right to opt-out of such disclosure. The carrier must enter into confidentiality agreements with its independent contractors and joint venture partners that prohibit additional use or dissemination of the individually identifiable CPNI by the contractor or joint venture partner.
- Carriers must obtain a customer's express, opt-in approval to disclose a customer's individually identifiable CPNI to third parties or to use it to market non-communications-related services or goods.

#### **D. Our Overall Approach**

28 Stakeholders have alternatively urged us to adopt across-the-board opt-in and across-the-board opt-out requirements for telecommunications companies' use of customer information. Others have urged us to defer completely to the rules adopted by the FCC, either by not adopting any rules or by adopting rules identical to the FCC's.

29 We reject the suggestion that we adopt without change all of the FCC rules. We consider a record different from the FCC's. We consider state as well as federal law in our decisions. Washington state stakeholders expressed to us views that were different from those heard by the FCC. And—perhaps because we are closer to our customers than is the FCC—we weigh factors differently from the balance implicit in the FCC rules. Like the FCC, we adopt a combination of opt-in and opt-out protections. Our rules, however, require

express (opt-in) approval from customers in more circumstances than do the FCC's rules. We adopt these additional protections based on the extensive record in this docket, and on our consideration of federal as well as state law.<sup>10</sup>

30 The sources of our authority to make rules on this subject are RCW 80.01.040(3) and RCW 80.36.140, which authorize us to regulate, in the public interest, the practices of telecommunications companies on a broad range of matters. Unlike the FCC, we are not bound by the 10<sup>th</sup> Circuit's decision. We nonetheless acknowledge the importance of taking care that our regulations do not unnecessarily restrict companies' protected commercial speech with their customers.

31 Qwest, Verizon, Sprint, and others, have presented arguments that they are entitled, in the exercise of commercial free speech protected by the Constitution, to use information in their possession about their customers to communicate with their customers or others, i.e., to solicit buyers for the services that they provide. In order to address these commercial free speech arguments, we have used the same analytical framework the FCC used in its August 2002 rule adoption order. That analysis is derived from the U.S. Supreme Court's *Central Hudson*<sup>11</sup> decision.

32 We assume, for the purpose of designing our rules, that a telecommunications company has an interest, protected by the First Amendment, in proposing lawful commercial transactions to its customers, in a non-misleading manner, on the basis of its knowledge about services to which those customers already subscribe from the company. At the same time, we are mindful of customers' interests in their privacy, in their free speech rights, and in their right to associate freely with others. These interests, too, are protected by our state and federal constitutions and underlie the state and federal laws we consider here.

---

<sup>10</sup> 47 U.S.C. § 222; U.S. Const. Amend. I; U.S. West v. F.C.C., 182 F.3d 1224 (10<sup>th</sup> Cir. 1999); RCW 80.01.040; ch. 9.73 RCW; Wash. Const. Art. 1, §§ 5, 7; In the Matter of Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers, Third Report and Order and Third Further Notice of Proposed Rulemaking (Released: July 25, 2002).

<sup>11</sup> *Central Hudson Gas & Elec. Corp. v. Public Service Comm'n of N.Y.*, 447 U.S. 557, 564-65 (1980)(setting out the test to be applied in determining whether restrictions on commercial speech survive “intermediate scrutiny”).

- 33 In part II, below, we identify the interests we seek to protect and explain why we find they are “substantial” interests to which commercial speech interests may be required to yield. Our conclusions are based on our view of the pertinent law. They are supported by comments we received from consumers in response to the Qwest opt-out notice, on comments received from stakeholders in this rulemaking, and on privacy values related to telephonic communications that are expressed in the statutory and constitutional law of our state.
- 34 In part III, below, we explain how our rules directly and materially advance protected privacy and free speech and association interests and why the means we have chosen are carefully crafted to impinge on any freedoms no more extensively than necessary. We weigh the relative merits of “opt-in” and “opt-out” privacy protections by considering information in comments, including polling data and expert analysis related to consumers’ experience with opt-out privacy notices in other industries, as well as consumer and stakeholder comments related to Qwest’s recent opt-out notice.
- 35 While we are cognizant of telecommunications companies’ commercial free speech interests, we weigh these interests against very important constitutional values on the customer’s side of the equation. One’s ability to keep private those communications that one chooses (and in which one has a reasonable expectation of privacy, supported by existing law) serves vital constitutional values of privacy and free speech and freedom of association. Perhaps it is obvious, but the telephone is used for *private communications* with *others*. It is thus an instrument by which these important and protected interests are achieved. While we recognize that, at some point, an advance in customers’ privacy interests may represent a diminution in companies’ commercial speech rights, we cannot ignore that the converse is also true: an increase in commercial usage of customer’s CPNI at some point represents a decrease in the protection of the customers’ interests.
- 36 We have sought to develop rules that are consistent with the U.S. Constitution, with Section 222 and the FCC’s rules interpreting that statute, and with our own state laws and constitution. While we respect the FCC’s approach to this topic, we nonetheless make our own findings about the kinds of interests we seek to protect and the balance we find it necessary to strike between consumers’ interests and companies’ interests.

37 On the totality of these considerations, we find that the FCC's rules leave certain substantial privacy, free speech and free association interests inadequately protected in Washington State. As the FCC anticipated and expressly allowed in its order, we conclude that the provisions of law we are entitled and required to consider and the record before us require us to provide safeguards more stringent than those required by the FCC's rules.

## **II. MAINTAINING THE STRICTEST CONFIDENTIALITY OF AN INDIVIDUAL'S COMMUNICATIONS OVER THE TELEPHONE IS A SUBSTANTIAL STATE INTEREST.**

### **A. Because of the nature of services they provide, telecommunications companies are necessarily engaged in full-time monitoring of private communications.**

38 As the owners and operators of telecommunications lines, telecommunications companies might be said to be engaged in full-time "wiretapping" of the phones or equipment that connect to their lines.<sup>12</sup> The wiretapping laws plainly extend to carriers insofar as carriers might attempt to listen in on phone calls or otherwise intercept the content of what they carry. But additional personal information is acquired in setting up calls and billing for them. As we will discuss below, the wiretapping laws cannot include any blanket prohibition on the acquisition, storage, and use of such information, because it is not possible to run a phone network without it.

39 Telecommunications carriers possess the capability to track certain information that results when subscribers use their telephones. Some of these tracking methods are commonly used (e.g., tracking long-distance calls for billing), while others may be used less frequently (e.g., tracking local dial-up calling to Internet service providers).

40 The technical capability of telecommunications companies to trace and track calling habits, and specifically to identify where and to whom the calls are being placed, has resided in the software of electronic network equipment for a

---

<sup>12</sup> *Huber, Kellog, and Thorne, Federal Telecommunications Law*, §14.5.2, 2d Ed. (1999).

number of years. Although historically the primary use of the information companies collected was for forecasting growth and engineering the network to handle peak loads, recent federal legislation has required companies both to extend the types and amounts of information gathered, and to make this information available to government entities in certain situations.

41 With the passage of the Communications Assistance for Law Enforcement Act, or CALEA, in 1994, a telecommunications company is required to:

[E]nsure that its equipment, facilities or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications, are capable of :

- (1) expeditiously isolating and enabling the government, pursuant to a court order, to intercept...all wire and electronic communications carried by the carrier...[and]
- (2) ...to access call identifying information...
  - (A) before, during, or immediately after the transmission...

*CALEA, Sec. 103 (a).*

42 In Section 102 (2) of CALEA, “call identifying information” is defined as information from dialing or signaling that identifies “origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment.”

43 Under the requirements of CALEA, a telecommunications company must at least have the capability to take the following actions:

- Track local calls
- Track long distance calls
- Track feature use
- Track answer or no answer
- Track three-way calling
- Track conference call participation
- Track 800 calls
- Track 900 calls

- Track length of local calls
- Track local dial-up Internet by ISP

For billing purposes, local service providers also record information regarding the length of long distance calls (regardless of long distance carrier) that originate and terminate on their switches. They may also track the number of rings before a phone is answered, either to start the billing of the long distance call, or in order to forward an unanswered call.

44 While a telecommunications company might not actually use all of this information on a day-to-day basis, and might not even track a customer's usage regularly, the technical capability to collect the information is certainly available. Without certain restrictions, the companies potentially could use the information for marketing or other purposes.

**B. The development of a marketing database industry has turned private information in the possession of any business, including telecommunications companies, into a potential source of revenue.**

45 Many believe, with good reason, that we are lately experiencing an erosion of our private sphere—not at the hands of government, but at the hands of private enterprise. Advances in information technology and the search for improved efficiencies in productivity, which we herald in other contexts, are driving the trend.<sup>13</sup> As stated in a research paper prepared under auspices of the Washington State Attorney General and the University of Washington School of Law:

The information revolution, the affiliation of previously unrelated types of businesses, as well as the growth of data mining<sup>14</sup> and

---

<sup>13</sup> Scholars have foreseen the threat that database technology poses to personal privacy for some time. “[M]any people have voiced concern that the computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been stored in it, may become the heart of a surveillance system that will turn society into a transparent world in which our homes, our finances, and our associations will be bared to a wide range of casual observers, including the morbidly curious and the maliciously or commercially intrusive.” A. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* 3 (1971).

<sup>14</sup> A standard definition for data mining is the non-trivial extraction of implicit, previously unknown, and potentially useful knowledge from data. Another definition is that data mining is a variety of techniques

target marketing have contributed to a change in data collection. A consumer's personal information has the potential of being bought and sold like any other valuable commodity.

\* \* \*

46 There are currently more than one thousand companies compiling comprehensive databases about individual consumers, a ten-fold increase in just five years.<sup>15</sup> Rather than engaging in mass marketing, they focus on gathering as much information as possible about specific people to engage in targeted or “profile” marketing. By compiling layer upon layer of information about specific individuals, they are able to produce a profile based on income, lifestyle, and an enormous variety of other factors.<sup>16</sup>

Using these databases, it is possible to identify people by what many would consider private aspects of their lives, including their medical conditions, their SAT scores, and their ethnicities.<sup>17</sup> Those selected by their personal characteristics can be targeted not only by direct marketers, but also by lawyers, insurance companies, financial institutions, and anyone else who has the funds to pay for the information.<sup>18</sup>

47 In short, there is an emerging market for information that may be used to predict individual consumers' receptiveness to offers of particular products and services. We are concerned that telecommunications companies, in their efforts to find new sources of revenue, may wish to sell or make other financial

---

used to identify nuggets of information or decision-making knowledge in bodies of data, and extracting these in such a way that they can be put to use in areas such as decision support, prediction, forecasting, and estimation. See <http://www.dacs.dtic.mil/databases/url/key.hts?keycode=222> (this explanation and citation is contained in the original research paper).

<sup>15</sup> Mike Hatch, *Electronic Commerce in the 21<sup>st</sup> Century: the Privatization of Big Brother: Protecting Sensitive Information from Commercial Interests in the 21<sup>st</sup> Century*, 27 *Wm. Mitchell L. Rev.* 1457, 1471 (2001) citing Robert O'Harrow Jr., *Data Firms Getting Too Personal?*, (*Wash. Post*) March 8, 1998 at A-1 (this citation is contained in the original research paper).

<sup>16</sup> *Id.* at 1471 (citation is contained in the original research paper).

<sup>17</sup> *Id.* at 1471 (citation is contained in the original research paper).

<sup>18</sup> Sellis, Ramasastry, Kim, and Smith, *Consumer Privacy and Data Protection: Protecting Personal Information Through Commercial Best Practices*, pp. 9-10 (2002).



use of records about customer communications. As described above, because of the nature of the services they provide, telecommunications companies have a window on a large amount of very personal and potentially very telling information about their customers. We find that it is therefore imperative to clarify, in the face of this potential source of revenue, that certain information about customers' communications patterns is off-limits to marketing use and disclosure to third parties, at least without the customers' express approval.

48 Finally, we observe that the ready commercial availability of call detail would make a mockery of protection of that same information from use by government: in the pursuit of compelling state interests such as the prevention and prosecution of crime, individual law enforcement agents and agencies of government could obtain the information not only by presentation of a search warrant authorized by a judge but also merely by purchasing it from the company or from any of a number of other commercial database suppliers.

**C. The potential harm from use and disclosure, without consent, of individually identifiable call detail information is significant.**

49 We embrace the FCC's objective of giving consumers a realistic opportunity to control the disclosure of information about themselves to parties outside of the telephone company. But to this we add a second objective of our own: that of curbing, even *within* the company, the creation of intrusive new profiles of individuals' communications patterns from what would otherwise be anonymous data. We explain both of these objectives in turn below.

**1. Without express consent, the disclosure of call detail could cause embarrassment, pecuniary loss, or a threat to safety.**

***Fear of disclosure could chill citizens' use of the telephone to freely speak and associate with others.***

50 Washingtonians have long relied on the assumption that records of whom they call and who calls them will be used only as necessary to provide the service to which they subscribe or to bill them for toll service. It is important to consider

the exact interests that would be harmed by the disclosure of this type of information, which we define as “call detail.”

51 Justice Stewart, in a dissenting opinion to *Smith v. Maryland*, 442 U.S. 735, 748 (1979) stated this interest succinctly:

Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and places called, and thus reveal the most intimate details of a person's life.

52 The specific kinds of potential harm of such disclosure are limitless, but a few examples are illustrative:

- People who wish to remain anonymous for their own safety—such as people who are subject to abuse or stalking or who might be sought for retaliation—could be endangered if it were possible for others to obtain lists of calls by or received by such person's relatives.
- People could be screened by prospective employers or fired from their jobs based on perfectly lawful communications with people or organizations to which their prospective or current employers object.
- Candidates for political office could face unfair scrutiny based on associations with organizations and people with whom telephone records indicate they or their family members have communicated.
- People wishing to intimidate or harass members of particular political causes, lifestyles or practices, or religions, could obtain organizations' calling records and with the help of a reverse telephone directory, determine the names and addresses of people connected with such causes, practices, religions, etc.
- Reporters could have sources compromised, despite assurances that the sources would remain anonymous.

- Firms could gain insights into their competitors' trade secrets such as the identity of suppliers, call volumes, and, with the aid of a reverse directory, the identity of a competitor's customers.
- With data about answered/unanswered calls, thieves could find out when an individual is likely or unlikely to be home.

53 Aside from these specific kinds of harm, there would also be a more generalized, but profound, harm to all of us, and to society. The ability of individuals to keep their personal communications private is a bedrock value, protected by our federal and state constitutions in several ways. Privacy interests are protected, as are free speech and association interests. Private free speech and association might be said to be triply protected. The primary purpose of a phone, after all, is to communicate with another person. If citizens fear that their use of the telephone will result in disclosure of very personal information, they will be reluctant to *use* the telephone for its intended purpose: *speaking to others*.

54 The instances listed above are all examples of harm that could result from disclosure of private call detail outside the telecommunications company. Every party to this rulemaking appears to concede that protection from these kinds of harm represents a substantial interest.<sup>19</sup> Many telecommunications company commenters stated that they *do not* currently disclose individually identifiable CPNI, which includes what we define as call detail information, to third parties. None stated they do make such disclosures.

55 We conclude that these kinds of potential harm are grave enough that companies should not be allowed to assume consumer consent for disclosure of call detail to third parties without explicit "opt-in" approval from the customer.

---

<sup>19</sup> The court in *U.S. West* expressed some concern about the FCC's articulation of this interest, but ultimately assumed that the government had asserted a substantial interest in protecting people from the disclosure of such information. *182 F.3d at 1235-36*.

**2. Even within a company, call detail is too sensitive to be used for profiling or targeted marketing, without a customer's express consent.**

56 The consumer interests discussed above could be protected, to some degree (though in our view not adequately<sup>20</sup>) by a rule that simply prohibits disclosure of call detail outside the company—or perhaps more broadly, outside the “corporate family.”

57 Even if it were possible, however, to devise a reliable system to ensure that call detail information would not be used in a way that results in any of the types of harm mentioned above, but only to develop profiles of individual consumers for direct marketing by the company that serves them, there would still be the potential for a serious and substantial invasion of privacy,<sup>21</sup> with its consequent effects on other interests.

58 To be clear, our goal is not to curb marketing *per se*. We accept the premise that as consumers, we benefit when producers, as a result of knowing something about prior purchases we have made, are better able to inform us of goods and services that might be of use to us, thereby allowing us to make better-informed purchasing decisions. However, where some kinds of information are concerned, this benefit is outweighed by consumers' unwilling loss of control over what they wish to reveal about themselves and for what purposes.

59 One consumer advocate recently described the types of privacy invasions that could result in the absence of rules prohibiting access to call detail:

A consumer desiring a phone number must give personal information to the phone company. Information thereafter is developed from the consumer's phone patterns, such as whether

---

<sup>20</sup> We are concerned that the risk of harmful disclosure we describe in the preceding section would increase if call detail information were permitted to flow to additional company personnel or company agents or contractors for the purpose of developing profiles of individuals for targeted marketing purposes.

<sup>21</sup> By privacy, we mean the interest in controlling disclosures of private information about oneself. We do not use the word to refer to the interest in not being bothered in one's home by sales calls. Consumers have other legal tools at their disposal to deal with the latter kind of privacy invasion. See *RCW 19.158.110(2)*, which provides that if recipient of a telemarketing call indicates she does not want to be called again, the marketer must not call again for at least one year and may not sell or give the person's name and number to other marketers.

the individual makes calls during the workday or calls certain phone numbers, like pizza delivery, on certain days and times of the week. Certain repetitive calls, such as regular calls out-of-state, can give clues as to the location and behavior patterns of family members. The frequency and duration of telephone calls to health care or insurance providers can give important clues about a family's health concerns. An observer can run consumers' call patterns through computerized screens to find consumers with "desirable" behavior patterns. Only the observer's ethic will limit the ends and means for using the information. More importantly, a company can secretly target the consumer without revealing how extensively these phone patterns made the consumer's personal life an open book.<sup>22</sup>

60 A group of state attorneys general expressed similar concerns to the FCC in the wake of Qwest's issuance of its poorly received opt-out notice in January of 2002:

While the carriers might not disclose this highly valuable information to their competitors, they would disclose this information to marketing partners for the purpose of jointly marketing products and services unrelated to the customers' current service selection and even unrelated to telecommunications services entirely. For instance, carriers could enter into joint marketing arrangements with providers of certain types of medical products, and send solicitations to the homes of customers who call certain types of doctors or other health care providers. Similarly, carriers could enter into contractual arrangements with telemarketers to sell the telemarketers the names of customers who call certain retailers, or who access the web for a certain period of time or at a certain time of day. The type of information that telemarketers and joint marketing partners would find useful, and therefore be willing to pay for, is limitless. Telemarketers would use this infinite variety of CPNI information in selecting targets for an infinite variety of

---

<sup>22</sup> Letter dated May 29, 2002 to the Utilities Division of the Arizona Corporation Commission from Lindy Funkouser, Director of Arizona's Residential Utility Consumer Office, quoted at p. 15 of *Comments of Public Counsel, Attorney General of Washington* (May 22, 2002) in this proceeding.

solicitations, and the carriers would generate new sources of income from this resource. The only party to the transaction that will not have consented, and will not necessarily benefit, is the customer.<sup>23</sup>

61 The FCC's rules attempt to address the threat of this kind of invasive monitoring. They do so by restricting the use of information that is obtained without express, opt-in customer approval to the marketing of *communications-related* services and they require companies to limit their affiliates, independent contractors, and joint venture partners to this use of CPNI by contract. 47 *C.F.R. § 64.2007(b)*. We choose, for the reasons stated above, to require opt-in approval for *any* use of call detail information. Also, as we will explain, we draw the definition of the corporate family (outside of which the company may not disclose a customer's CPNI without express approval) more narrowly.

62 The technology of telecommunications, and federally-mandated identification and preservation of calling information, give telephone companies access to more intimate information about their customers than most other businesses possess. Telecommunications companies are in a position similar to that of health care providers, insurance companies, some kinds of financial institutions, cable providers, and video stores, in that they are in a position to gain a window on sensitive information about individual customers.<sup>24</sup>

---

<sup>23</sup> *Letter dated December 21, 2001, from 39 Attorneys General, to Federal Communications Commission, In matter of Telecommunications Carrier's Use of Customer Proprietary Network Information, CC Docket No. 96-115 and 96-149.* For many years, Judge Greene invoked concerns about misuse of customer information as a reason to bar phone companies from providing online information services of any kind. Although Judge Green was concerned about competitive issues, his concerns also have a strong privacy dimension. Through "control of its customers' lines of communication," a local phone company would "also have access to their lines of credit, travel plans, credit card expenditures, medical information, and the like. On the basis of a subscriber's telephone calling patterns with respect to information, an RBOC [Regional Bell Operating Company] could easily pinpoint that subscriber for the sale of RBOC-generated information and the sale of other products and services connected therewith, to the point where that company would have a 'Big Brother' type relationship with all those residing in its region." *United States v. Western Elec. Co.*, 6763 F. Supp. 525, 567 n. 190 (D.D.C. 1987), *rev'd in part, aff'd in part*, 900 F.2d 283 (D.C. Cir. 1990); *see also United States v. Western Elec. Col.*, 714 F. Supp. 1, 12 n. 40 (D.D.C. 1988) (*Bell companies barred from offering "user profile" services*).

<sup>24</sup> Incumbent local exchange carriers ("ILECs")—the most outspoken opponents of rules requiring express customer approval for the use of private information—are different from these other kinds of businesses in a significant way: their customers do not, in most cases, have the ability to choose another provider who will respect their privacy wishes.

Lawmakers have acted in fields such as these,<sup>25</sup> to ensure the confidentiality of particularly sensitive information. As we will discuss below, lawmakers in this state have acted also in the field of telecommunications privacy.

63 Unlike the FCC, we are concerned that a significant privacy interest, recognized by our state law and within the reasonable expectations of Washington consumers, would be compromised by a rule allowing a telecommunications company to engage in data mining and profile-building of its customers' communications patterns, even if only for the company's own targeted marketing purposes. To provide some specific examples, we find that the following practices, described either as a hypothetical possibility or as a current practice by commenters in this rulemaking, are too invasive of customer privacy to allow unless the company first obtains express customer approval:

- Monitoring customers' hourly, daily, or weekly call volumes and calls answered/unanswered, for use as a tool in approaching the customers and selling particular services to help them better manage their telecommunications. *Qwest's April 12, 2002 comments at page 6.*
- Monitoring customers' called telephone numbers to identify customers who might be receptive to an optional toll plan that offers a flat rate for calls made to other customers of that company. *Verizon's May 22, 2002, comments at page 9.*
- Monitoring the monthly amount a customer spends calling a particular area code to develop a sales lead list of customers who might be receptive to a plan that has special rates for calls made to a particular area code. *Sprint's May 22, 2002 comments at page 2; WITA's May 17, 2002 comments at page 2.*

---

<sup>25</sup> *Cable Communications Policy Act of 1984 (47 USC §521 et seq., §611); Video Privacy Protection Act of 1988 (18 USC §2710, §2711); Privacy of Consumer Financial and Health Information, Chapter 284-04 WAC; Fair Credit Reporting Act (15 USC §1681 et seq.); See also, Gramm-Leach-Bliley Financial Modernization Act (15 U.S.C. § 6801); Electronic Communications Privacy Act of 1986 (18 USC §1367, § 2232, §2510 et seq., §2701 et seq., §3117, §3121 et seq.); Electronic Fund Transfer Act (15 USC § 1693); Communications Assistance for Law Enforcement Act of 1994 (47 USC §§1001-1-10; §1021; 18 USC §2522); Driver Privacy Protection Act of 1994, and as amended in 1999 (18 USC §§2721-2725); Family Education Rights and Privacy Act of 1974 (20 USC §1232g); Federal Privacy Act (5 USC §552a); Right to Financial Privacy Act of 1978 (12 USC §3401 et seq.).*

64 We find that these uses of call detail constitute a privacy invasion for which a company should be required to obtain express, opt-in customer consent. The creation of these profiles without customer consent is, in itself, an invasion of privacy, even if the information never makes it into the hands of a third party. We are also concerned that such practices increase the risk that companies will unintentionally disclose very sensitive information to third parties through dishonest company agents or employees, or through negligence.<sup>26</sup> In other words, part of our objective is to allow customers to control the creation of new points of exposure to their privacy.

65 Also, as we have earlier observed, if customers fear an invasion of privacy when they use the telephone, they are less likely to use the telephone to speak to and associate with others. We do not want to adopt rules that would chill these activities.

**D. Under existing Washington law, it is well established that telecommunications companies hold telephone calling records for a limited purpose—to deliver service and to bill for it.**

66 Under Washington statutes it is both a criminal offense<sup>27</sup> and a basis for civil liability<sup>28</sup> for anyone to intercept or record private communications transmitted by telephone without obtaining the consent of all the parties to the communication prior to each such interception or recording.<sup>29</sup> Washington's

---

<sup>26</sup> Our record includes numerous complaints that opt-out directives to Qwest in January and February of this year were not recorded by company staff. At issue was protecting customer information from disclosure to third parties, according to Qwest's opt-out notice, "when it is commercially reasonable to do so."

<sup>27</sup> Under RCW 9.73.080, anyone who violates RCW 9.73.030 is guilty of a gross misdemeanor.

<sup>28</sup> RCW 9.73.060 provides: "Any person who, directly or by means of a detective agency or any other agent, violates the provisions of this chapter shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this statute has injured his business, his person, or his reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him on account of violation of the provisions of this chapter, or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a reasonable attorney's fee and other costs of litigation."

<sup>29</sup> RCW 9.73.030 provides: "(1) Except as otherwise provided in this chapter, it shall be unlawful for any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept, or record any:

(a) Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any



prohibition on violating a person's right to privacy is similar, but not identical to federal statutes pertaining to wiretapping of interstate and foreign communications.<sup>30</sup> Both Washington and Federal law plainly extend to phone companies,<sup>31</sup> particularly insofar as a company might attempt to listen in on phone calls or otherwise intercept the content of the calls they carry.<sup>32</sup>

67 As a matter of obvious necessity, however, there are some broad exceptions under state and federal criminal statutes for the activities of telecommunications companies. Most importantly, Washington's statutory prohibition on intercepting or recording such communications does not apply to:

any activity in connection with services provided by a common carrier pursuant to its tariffs on file with the Washington utilities and transportation commission or the Federal Communication Commission and any activity of any officer, agent or employee of a common carrier who performs any act otherwise prohibited by this law in the construction, maintenance, repair and operations of the common carrier's communications services, facilities, or equipment or incident to the use of such services, facilities or equipment.<sup>33</sup>

---

device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication”

<sup>30</sup> See 47 USC § 605(a) (“no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels . . .”)

<sup>31</sup> For example, in *State v. Riley*, 121 Wn.2d 22 (1993), a criminal defendant alleged that US WEST had violated the statute by using a trace device to identify the number from which someone was repeatedly placing calls to the access number of a long distance provider in an apparent attempt to discover the access codes of the long distance provider's customers. US West gave the information to police and the police used it to obtain a search warrant, but the court analyzed whether US WEST had violated the law. The court found it had not because either (1) a tracer device does not intercept a “private communication” within the meaning of the act, or assuming it does (2) it was nonetheless permissible for the phone company to establish a line trap to trace hacking activity as part of its “operations” under RCW 9.73.070. The legislature later amended ch. 9.73 RCW to extend the protections of the statute to “the originating number of an instrument or device from which a wire or electronic communications was transmitted”—the information recorded by a trap and trace device like the one at issue in *Riley*. RCW 9.73.260; 1998 Wash. Laws ch. 217, sec. 1.

<sup>32</sup> Huber, Kellogg, Thorne, *Federal Telecommunications Law*, 2<sup>nd</sup> Ed., § 14.5.2 (1999).

<sup>33</sup> RCW 9.73.070(1).

68 An important way in which the federal wiretap law and Washington's privacy law differ is in how they treat information of the type contained in toll records. Federal courts have held that a phone company's disclosure of a customer's toll records, including numbers called and the length of the conversation (again, what our rule would label "call detail"), is not a violation of the federal wiretap statute.<sup>34</sup> By contrast, as the Washington Supreme Court has stated:

The State of Washington has a long history of extending strong protections to telephonic and other electronic communications. For example, RCW 9.73.010, which makes it a misdemeanor for anyone to wrongfully obtain knowledge of a telegraphic message, was enacted in 1909 and is based on section 2342 of the Code of 1881. The 1881 Code, adopted before statehood, extensively regulated telegraphic communications. See Code of 1881, §§ 2342-62. Our present statute is broad, detailed and extends considerably greater protections to our citizens in this regard than do comparable federal statutes and rulings thereon.<sup>35</sup>

69 Under Washington statutes, the kind of "communications" that are not to be intercepted include not just the content of the conversation between the parties, but also the simple act of dialing from one telephone number to another.<sup>36</sup>

70 RCW 9.73.260 specifically provides that a court order is required for any person to use a "pen register" (a device that identifies all outgoing local and long distance numbers dialed, whether the call is completed or not) or a "trap and trace device" (a device to record the number of an incoming call) on someone's phone line, and only law enforcement officers may petition for such orders.<sup>37</sup>

---

<sup>34</sup> See, e.g. *U.S. v. Baxter*, 492 F.2d 150 (9<sup>th</sup> Cir. 1973).

<sup>35</sup> *State v. Gunwall*, 106 Wn.2d 54, 66.

<sup>36</sup> Private communication under RCW 9.73 includes "the dialing from one telephone number to another." *State v. Riley*, 121 Wn.2d 22, 34 (1993); *State v. Gunwall*, 106 Wn.2d 54, 69 (1986).

<sup>37</sup> Again, telecommunications companies' equipment is necessarily exempted from the definition of pen register:

such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or

71 Unlike its federal counterpart, Washington’s law does not specifically prohibit divulging or disclosing communications; it only prohibits intercepting or recording them. As noted above, to the extent phone companies intercept or record such information in connection with the delivery of telecommunications services, the law does not apply to them. It could plausibly be argued that because there is no specific prohibition on *disclosing* such records, it would not be unlawful for the phone company to *use*, for any purpose that is not otherwise prohibited, call detail information that it has already recorded in the ordinary course of providing telecommunications services. We find that such an interpretation would be contrary to the privacy interests our legislature sought to protect in enacting laws to protect the privacy of telephonic communications. Part of our intention in adopting these rules is to fill the gaps between Washington’s statutory protections on the privacy of communications and the FCC’s CPNI framework.

72 Article I, Sec. 7, of the Washington Constitution<sup>38</sup> prohibits intrusions of privacy by the government of the sort that our rule prohibits for telephone companies. The Washington Supreme Court has held that the government may not obtain toll records and may not use a pen register without valid legal process such as a search warrant issued on probable cause. In so holding, the Washington Supreme Court quoted, as part of its reasoning, the words of the Colorado Supreme Court in finding a similar right to privacy:

A telephone subscriber . . . has an actual expectation that the dialing of telephone numbers from a home telephone will be free from governmental intrusion. A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one’s ability to effectively communicate in today’s complex society. When a telephone call is made, it is as if two people are having a conversation in the privacy of the home or office, locations entitled to protection under . . . the Colorado

---

customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

RCW 9.73.260(1)(d). What is noteworthy about this exemption, like the more general exemption discussed above, is that it is not a blanket exception for phone companies, but an exception the companies are allowed for a limited purpose—specifically, billing and accounting.

<sup>38</sup> *Article I, Sec. 7, Wash. Const.* reads as follows: “Invasion of private affairs or home prohibited. No person shall be disturbed in his private affairs, or his home invaded, without authority of law.”

Constitution. The concomitant disclosure to the telephone company, for internal business purposes, of the numbers dialed by the telephone subscriber does not alter the caller's expectation of privacy and transpose it into an assumed risk of disclosure to the government.<sup>39</sup>

73 To be clear, we recognize that search and seizure law is concerned with intrusions of privacy by the government—not by private enterprise. We nonetheless find the courts' analyses and holdings in these cases to be relevant to our analysis. In determining the extent of the Fourth Amendment's protection against warrantless searches, and the Washington Constitution's prohibition against being disturbed in one's private affairs, courts have been called upon to define the sphere within which a citizen has a "reasonable expectation of privacy."<sup>40</sup> We find this "reasonable expectation of privacy" inquiry to be much closer to the mark of what constitutes a substantial interest for First Amendment purposes than the apparently more restrictive test posited in Qwest's comments. Qwest suggests that we have a substantial interest (within the meaning of the *Central Hudson* test of regulatory burdens on commercial speech) only in protecting information that, if disclosed, would be "highly offensive" to a reasonable person to whom it pertained. *Qwest comments of March 21, 2002, p. 11.*<sup>41</sup> Qwest notes that this is the standard for the tort of

---

<sup>39</sup> *State v. Gunwall*, 106 Wn.2d 54, 67 (1986), citing *People v. Sporleder*, 666 P.2d 135, 141 (Colo. 1983).

<sup>40</sup> *See Katz v. U.S.*, 389 U.S. 347 (1967).

<sup>41</sup> Qwest also points out that this is the statutory standard for determining whether someone has a right to privacy in a particular piece of information, held by the government, that is sought for disclosure under Washington's Public Disclosure Act (PDA), *RCW 42.17.250, et seq.* The *RCW 42.17.255* standard for determining whether there is a right to privacy in information sought for disclosure is "if disclosure of information about the person: (1) would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public." We find this too narrow a standard for our "substantial interest" analysis. The Public Records provisions of the PDA are suffused with the policy that citizens have a right to know what the governmental agencies they have created are doing. *RCW 42.17.251*. This "government in the sunshine" policy is so important that the drafters of the citizen's initiative, Initiative 276, chose to draw narrowly the individual's countervailing interest in the privacy of public records that pertain to himself or herself. We note, however, that when the purpose of a disclosure request under the PDA is merely commercial—as opposed to serving the central policy of open government—the privacy protections of the Public Disclosure Act are far broader. In fact, agencies are expressly not authorized to disclose lists of individuals when such lists are requested for a commercial purpose. *RCW 42.17.260(9)*. Moreover, the more specific disclosure exemptions/privacy protections of the PDA include information similar to what we seek to protect with our rules. *See e.g. RCW 42.17.310 (a)* (Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients), *(l)* (Any library record, the primary purpose of which is to maintain control of library materials, or to gain access to information, which discloses or could be used to disclose the identity of a library user),

invasion of privacy (“publicity given to private life”) under the Restatement (Second) of Torts at 652D. We do not read the 10<sup>th</sup> Circuit’s decision as circumscribing the government’s authority so narrowly as to allow us to place burdens only on company speech that would otherwise constitute a tort. A tort standard makes sense only when applied to the facts of a particular case.<sup>42</sup> Tort law is aimed at providing remedies for particular wrongs. Our rules necessarily have broader application because they are aimed at preserving customers’ privacy and freedom of speech and association by reducing the risk of the occurrence of such wrongs.

**E. Consumer comments following the Qwest opt-out notice reflect an expectation of privacy in telephone records.**

74 During the course of this rulemaking, Qwest Corporation began sending opt-out notices to its customers in Washington, as well as in the other thirteen states where it is the regional Bell operating company. Qwest’s notices required customers to opt-out if they wished to prevent use and disclosure of their personal account information, despite the opt-in requirements of Washington rules. Qwest’s tactics were widely reported in the radio, television, and newspaper media, and many customers objected. Specific customer objections will be discussed below, but the general sentiment of telecommunications customers was that personal account information should be protected unless the customer gives express permission for other uses. Customers also objected strenuously to the use of their private information by the telephone company itself to market other services to them.

75 The inescapable conclusion of the recent Qwest experience (consistent with the legal analysis of the preceding section) is that customers believe their telecommunications companies have a duty to protect private information about them. Customers were astonished and angered at the notion that their

---

(*nn*) (The personally identifying information of persons who acquire and use transit passes and other fare payment media including, but not limited to, stored value smart cards and magnetic strip cards).

<sup>42</sup> See e.g., *Hill v. MCI WorldCom*, 141 F.Supp.2d 1205 (2001) (Under Iowa law, telecommunications carrier's alleged disclosure of phone numbers and addresses of customer's friends to customer's ex-husband, who had previously stalked, threatened, and harassed customer, gave rise to claim for invasion of privacy based on the theory of publicizing private facts, where the facts disclosed would have been extremely embarrassing, highly offensive, and potentially dangerous to a reasonable person in customer's situation, and the information disclosed was not of a legitimate concern to ex-husband).

telecommunications company might be able to disseminate information about them based on the assumption of their consent.

76 Beginning in mid-December 2001, Qwest mailed a bill insert to its customers, purportedly putting them on notice that the company intended to use and disclose CPNI for marketing purposes. Customers who objected to this use of their private account information were told to contact the company to opt out.

77 Customers who understood the company's intended use of their information objected strenuously and loudly. During January 2002, newspapers in this state published many letters from consumers who argued that Qwest was abusing its position as their provider of local telephone service and violating the customers' privacy rights. Newspaper editorials chastised Qwest for failing to respect its customers' privacy and exhorted regulators to act firmly to stop the intended practices.<sup>43</sup> The WUTC received over 600 comments from customers. The customer response was extraordinary for the WUTC. To our knowledge, no policy issue has generated this many unsolicited comments from members of the public over any period of time, let alone in one month.<sup>44</sup>

78 Most of the customers who commented simply voiced their opposition to the Company's requirement that they opt out in order to avoid commercial use of their private information. Others went further and made statements such as: "This is invasion of privacy and I thought it was illegal." Similar statements were made by nearly every commenter who went beyond "I am opposed to opt-out." However, some commenters went still further and commented on the nature of the relationship between them and their telecommunications company.

79 Those who commented about the relationship were unanimous in what they said. With striking consistency, they stated that they view the relationship as a limited one in which they pay the company to provide telephone service and, to

---

<sup>43</sup> See, e.g., Elizabeth Hovde, *Phone Company Rings Customers' Bells: Will Qwest Ever Get the Voice Mail?*, *The (Vancouver, Washington) Columbian*, January 8, 2002; Editorial, *Make "Opt Out" Easier for Qwest Consumers*, *The (Tacoma, Washington) News Tribune*, January 9, 2002; Opinion, *Qwest's Train Wreck*, *The Seattle Times*, January 19, 2002.

<sup>44</sup> The only instance in which customer comments exceeded these in the space of a month was during a strike by the Communications Workers of America against U S WEST. The strike lasted a month and tens of thousands of orders went unfilled, with the result that 750 people without dial tone contacted the WUTC to complain.

the extent they must provide information to establish service or to complete a call (dial a number), they consider that the relationship does not entitle the company to do anything with that information but use it to provide service.

80 Some examples of what people stated in e-mails to the WUTC:

- When I subscribe to any service, whether it be the utility company, the gas company, or the phone company, I am providing information to them solely because they require it before they will provide a service to me.
- I need a telephone; therefore, I do business with Qwest. I did not ever grant them permission to make money off of me, to solicit from me, to provide information about me to anyone for any reason.
- They are providing us a service that we have contracted for. We are not here to provide them with unlimited information which THEY can sell to the highest bidder.
- We are paying them for phone service. Our phone usage is our private business.
- The individuals supplied the information to the respective company for the singular purpose to contract a business relationship with that company. All information should be held private between the participants of that business relationship.

81 One comment spoke directly to the issue of non-disclosure in business relationships:

My clients are major corporations. Every single one of them requires me to sign a non-disclosure statement prior to my even talking to them about how my services might help them. These non-disclosure statements also forbid me to discuss what the company is doing when using my services and what services I am providing them. If I did not sign those non-disclosure agreements, I would not be able to get any work.

Clearly, customers do not believe that their telecommunications company has, as an assumed or implied extension of the customers' purchase of service, permission to use or disclose the customers' CPNI as the company pleases. Neither do customers believe it is enough, with respect to all possible uses and all types of CPNI, that customers should only have notice and an opportunity to revoke such implied permission.

**III. OUR RULE IS NARROWLY TAILORED TO PROTECT CONSUMERS' PRIVACY AND FREE SPEECH AND ASSOCIATION INTERESTS WITHOUT UNDULY BURDENING LEGITIMATE COMMERCIAL SPEECH.**

82 Having defined the interests we aim to protect, we now turn to the means. Commenters have proposed two general methods for ensuring that a customer's private account information is not used or disclosed in a manner that is inconsistent with the customers' expectations or wishes: opt-in and opt-out. Opt-out (implied approval) is shorthand for a method in which companies provide a customer notice of what the company intends to do with information about the customer and the customer is presumed to have assented to the use unless he or she takes some action to revoke that presumed permission. In other words, the customer must "opt out" of the company's proposed plan to use or disclose the customer's information.

83 Opt-in (express approval) refers to a method of determining a customer's preference in which the company must convince the customer to take some affirmative step to register that approval of the use proposed by the company.

**A. The opt-out method places a lesser burden on companies' use of customer account information, but recent experiences with its use demonstrate that it needs improvement.**

84 The companies favor the use of the opt-out method. Qwest claims that of the two methods, opt-out is the only one that results in a large enough percentage of customer "approval" to justify the expense to the company of even trying to obtain such approval for marketing use. We are sympathetic to this problem in those circumstances in which it is unlikely that customers would strongly object, and might actually benefit from, the company's proposed use. The



FCC also found this argument compelling with respect to in-company marketing use of CPNI and consequently allowed opt-out for such uses as require any customer approval.

- 85 A fundamental difficulty to be overcome by opt-out regulations is that the companies responsible for implementing such regulations may have an incentive *not* to provide a notice that customers will actually recognize, take the time to read, understand, and easily register a disapproving response.<sup>45</sup> As a result, previous attempts at making opt-out schemes work have failed to some degree in (1) getting customers' attention,<sup>46</sup> (2) presenting them with their options in language they understand,<sup>47</sup> and (3) providing them with a simple manner of registering their disapproval, if they so choose.<sup>48</sup>
- 86 In light of comments and information presented by various commenters regarding recent experience under the Gramm-Leach-Bliley Act and our own

---

<sup>45</sup> *Comments of the Electronic Privacy Information Center (EPIC) of May 22, 2002, p. 4-5, 9-11.* However, as the Qwest experience shows, there is also good reason to avoid making customers so upset as to generate significant ill will.

<sup>46</sup> *Comments of EPIC of May 22, 2002, p. 9; Comments of Attorneys General to FCC of December 21, 2001 (attachment to Public Counsel Comments of January 31, 2002), p. 8* (referring to two surveys concerning Gramm-Leach-Bliley Act opt-out notices: American Banker's Association survey which found that 41 percent of customers did not recall receiving their opt-out notices, 22 percent recalled receiving them but did not read them, and only 36 percent reported reading the notice; and Harris Interactive for the Privacy Leadership Initiative survey, which indicated that only 12 percent of consumers carefully read the notices most of the time, whereas 58 percent did not read the notices at all or only glanced at them).

<sup>47</sup> *Comments of Attorneys General, p. 8* (referring to conclusions of readability expert Mark Hochhauser, Ph.D. that Gramm-Leach-Bliley opt-out notices, which are required under the law to be written in a "clear and conspicuous" manner have been unintelligible and couched in language several grade levels above the reading capacity of the majority of Americans).

<sup>48</sup> We note that those telecommunications companies that have sent opt-out notices have registered opt-out totals that are substantially lower than one would expect from polling data concerning Americans' attitudes about privacy. For example Verizon reports that only 2 percent of its customers, nationally, have opted-out. *Comments of Verizon of May 22, 2002.* Sprint reports that only 5.6 percent of its Washington customers have opted-out. *Comments of Sprint of March 26, 2002, p. 9.* By comparison, a survey that Qwest views as favorable to its advocacy for opt-out places the number of "privacy fundamentalists" in the U.S.—who presumably would opt-out of any kind of data sharing if they only knew how—at 24 percent of the population. More dramatically, a January 2002 Rocky Mountain Poll in Arizona revealed that only 3.7 percent of polled adults believed that Qwest was on the right track when it announced it would sell customer records unless customers took the initiative to contact the company and object within a specific period of time. *Comments of Public Counsel of May 22, 2002, p. 14.* The findings of this latter poll are consistent with our own observation of consumer reaction to the Qwest opt-out notice in our state. Similarly, in a statewide referendum in North Dakota in June, 2002, 72 percent of voters favored repealing a 2001 state law that let financial institutions share or sell customer information unless customers opted out. The repeal reinstated previous state law barring such sharing unless customers opted in. *Adam Clymer, North Dakota Tightens Law on Bank Data and Privacy, New York Times, June 13, 2002.*

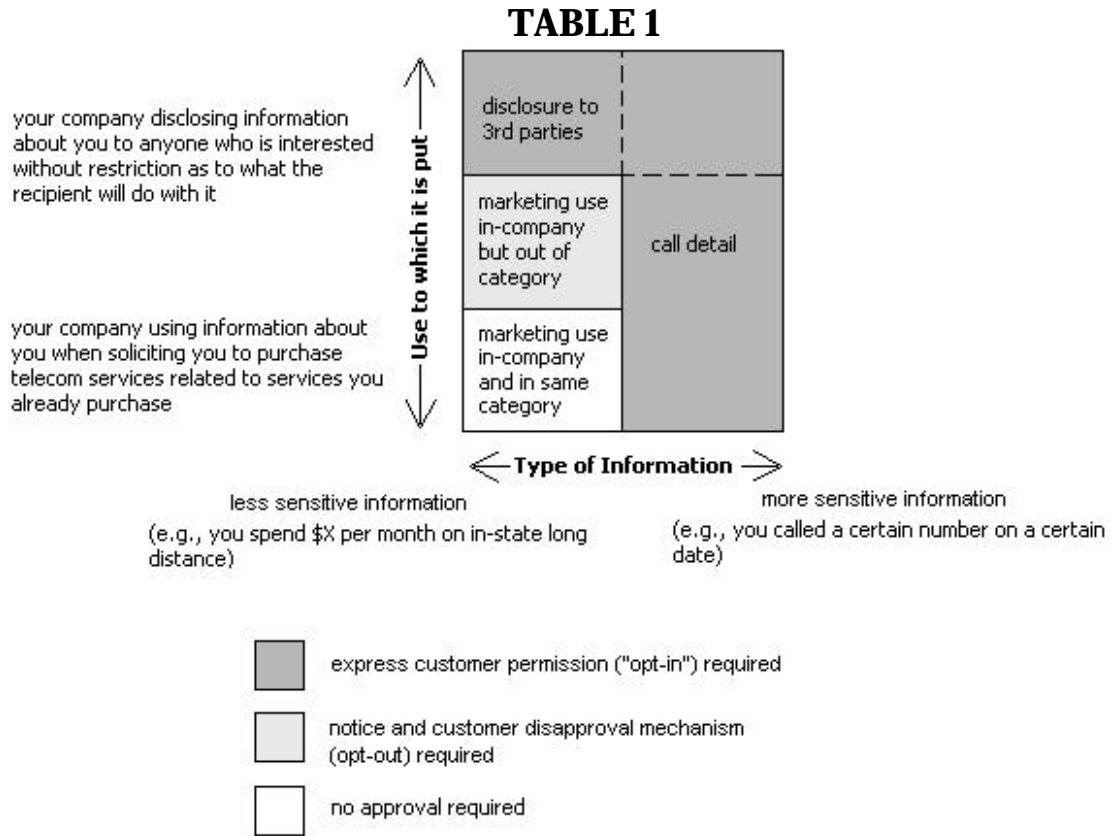
experience with the Qwest opt-out notice, we are adopting provisions to improve the visibility and content of the notices and to make it easier for customers to register their disapproval.

**B. Opt-in makes it more difficult for companies to obtain approval, but because it is less likely to result in accidental approval by the customer, it is appropriate for use where customers' privacy expectations are highest.**

87 A number of the telecommunications company commenters objected to an opt-in requirement because it puts the burden on the companies to overcome inertia by enticing customers with promises of specific benefits. We have no reason to doubt Qwest's assertion that it likely will not gain customers' opt-in approval in anything approaching the same numbers as through the opt-out method. We accept for argument's sake that many customers who might not actually object to the proposed use will not take the time to read such a solicitation and register their approval.

88 We find, however, that an opt-in approach is far less likely to result in the customer's accidental approval of the use of his or her private account information. For this reason, where the potential harm of unauthorized disclosure is most serious and where customers' reasonable expectations of privacy are most solidly rooted in existing law, we find it necessary to require companies to obtain customer's opt-in approval.

89 The schematic in Table 1 may be helpful to illustrate the consequences of our decision regarding where we find opt-in approval is necessary to protect customer's reasonable privacy expectation, where opt-out is sufficient in light of companies' commercial speech interests, and where no approval is necessary.



90 The whole box, in Table 1, represents the universe of individually identifiable customer proprietary network information and every use to which it might be put (aside from delivering service, billing for service, or responding to requirements of other applicable laws). The different degrees of shading in various parts of the box have the meaning set out in the key at the bottom of the illustration.

91 Imagine that the types of information that companies possess about their customers are arrayed on a continuum from the left to the right of the box, with the least "private" or sensitive at left edge and the most private at the right edge of the box. Next imagine that the types of uses to which the companies might put such information are arrayed on a continuum from the bottom to the top of the box. At the very bottom are those uses that are most likely to be within customers' expectations about how a company would use information about them and that are therefore unlikely to upset reasonable privacy expectations. At the top are those uses that a customer would least expect,

which would therefore be most upsetting to reasonable privacy expectations, and most chilling to the exercise of customers' free speech and association.

92 Unlike the FCC's rules, our rules acknowledge that some types of information are too sensitive or private for any use other than what is necessary to deliver and bill for service. The FCC's rules acknowledge only the dimension (uses of CPNI) that runs from bottom to top. Because of the breadth of the definition of CPNI,<sup>49</sup> we find it imperative to acknowledge the second dimension (i.e., from left to right of the box in Table 1).

93 We discuss our conclusions with respect to each of the shaded areas of this schematic in the sections that follow.

### **C. We require opt-in for any use of call detail information.**

94 Unlike the FCC, we require express, opt-in customer approval before a company may garner information about individual customers' *communications* patterns (as distinct from more generic information about their *purchasing* patterns) except as technologically necessary to provide service and billing. This requirement is represented by the dark-shaded portion on the right side of the box in Table 1. We apply this protection even if the company's sole purpose is to compile information for use in targeted marketing of its own services. To protect customers from this kind of intrusion without their consent we define a category of information known as "call detail." This is the information that commenters universally acknowledge to be the most sensitive or private information that companies possess about their customers.

95 Call detail includes any information about particular telephone calls, including the number from which a call is made, any part of the number to which it was made, when it was made, and for how long. It also includes aggregated information about telephone calls made to or from identifiable individuals or entities, and information about unanswered calls that is specific to a particular period of time. We carve out call detail for special protection because we find that the compilation of usage profiles from this information constitutes a

---

<sup>49</sup> The definition we adopt for CPNI inserts the words "including call detail" into Congress's definition, which already encompasses call detail. We insert the phrase so our rules are easier to follow where we treat only that subset of CPNI that is call detail—as distinct from "private account information," which makes up the other component of personally identifiable CPNI.

significant intrusion into the private affairs of the person who is the subject to the profiling. Expanding the permissible uses of this information to include marketing (as opposed to just technical processing and billing) would create new points of exposure and erode consumers' ability to control what information is revealed about them, and potentially chill their use of the telephone to speak to and associate with others.

96 We believe our protection of call detail is necessary for the protection of values that have long been established in Washington statutes and constitutional law. We find that Washington citizens have a right to expect greater protection of information about their communications over the telephone than the FCC's rules afford. By carefully tailoring our strongest protections for this sensitive information, we believe we have also met the requirement of federal statutes and the Constitution.

**D. We adopt opt-in for disclosure of individually identifiable CPNI outside the company.**

97 Like the FCC, we are adopting rules that require telecommunications companies to obtain express (opt-in) approval before the companies may disclose any non-public information about customers to unrelated third parties. This requirement is represented by the dark-shaded, upper portion of the box in Table 1. We have chosen, however, to define "third parties" more broadly (and thus the corporate "family" more narrowly) than the FCC. In our view, the FCC's inclusion of "affiliates," "independent contractors" and "joint venture partners" as part of the corporate family is overly broad, and the definition of joint venture partners is vague as well as broad. Also, we are not confident that companies will have adequate incentive to enforce the contracts that the FCC's rules require for the protection of CPNI in the hands of those affiliates and joint venture partners. The effect of our rule is to make disclosure to more kinds of companies subject to opt-in.

98 Although we emphasize in this order the special sensitivity of call detail information, we do not mean to suggest that individually identifiable CPNI other than call detail information does not need protection. For example, we think most customers would consider it a potentially serious invasion of their privacy for the phone company to sell a list of the telecommunications services the customer purchases, including the amount the customer spends each

month on those services, to any third party that would be willing to pay for the information. For many business customers, for example, this is commercially sensitive information. We therefore require opt-in approval before companies may disclose individually identifiable CPNI (including non-call-detail CPNI) to outside parties.

99 Consequently, our rules limit disclosure of private account information under the opt-out scheme to entities under common control with the telecommunications company that holds the information. We did not follow the FCC and permit access by “joint venture partners” to information that is subject only to the opt-out scheme, because that is a category that can fit any entity that uses information to market communications-related services. As a category, “joint venturers” is useless because it permits inclusion of every firm and excludes no firm. We find that such potentially broad disclosure, without express consent, is inconsistent with reasonable customer privacy expectations and we find little support in the *U. S. West* decision, or elsewhere, for the proposition that companies have a core commercial speech interest in selling such information to third parties.<sup>50</sup>

**E. We adopt opt-out for in-company use of (non-call-detail) private account information for the purpose of marketing services that are not within the same category of service to which the customer already subscribes.**

100 In our rules we define “private account information” as the subset of CPNI that does not include call detail but is associated with an identifiable individual. A company may rely on an opt-out notice when it proposes to use the customer’s private account information for its own marketing purposes (as opposed to selling the information or disclosing it outside of the company, which requires opt-in approval). This category is represented by the medium-shaded middle-left part of the box in Table 1.

101 Because the opt-out method, even with the improvements we are adopting, is still likely to be misunderstood or go unnoticed by at least some customers, we

---

<sup>50</sup> See *Trans Union Corp. v. Federal Trade Comm’n.*, 245 F.3d 809 (U.S.App. D.C. 2001), *cert den.* 122 S.Ct. 2386 (June 2002) (upholding rules adopted by Federal Trade Commission banning the sale of mailing lists by credit reporting agencies containing the names of consumers who met certain criteria, such as possession of an auto loan, a department store credit card, or two or more mortgages).

reserve its application to circumstances in which a failure to obtain informed consent is less serious and in which we find that most customers do not have a strong objection. For example, a company need only provide notice and an opportunity to opt-out before it may compile a targeted marketing list, for its own use, of its interexchange customers whose toll charges exceed a given amount per month.<sup>51</sup>

102 Aside from our opt-in restriction on call detail, our requirement of notice and an opportunity to opt-out for in-company use of private account information parallels the FCC's opt-out requirements, which the FCC arrived at based on section 222 and the record before it. As such, we see value in adhering to the general framework of the FCC's CPNI rules, when consistent with our own findings and record.<sup>52</sup>

103 Additionally, it is clear that in overturning the FCC's prior rules, the 10<sup>th</sup> Circuit was specifically concerned with restrictions on carrier speech that solicits a commercial transaction with the carrier's own customers and on speech within a company (including among affiliates) that facilitates that commercial solicitation. *U.S. West, 182 F.3d at 1233, fn. 4*. In such instances, *and* where concerns for the customers' privacy are less grave, it follows that our rules should have a lighter touch, though still preserving customers' opportunity to control the use of their private information.

**F. We do not require notice to customers before a company may use (non-call-detail) private account information to market services within the same category to which the customer already subscribes.**

104 Although we restrict access to call detail information for any purpose absent the customer's opt-in approval, we otherwise mirror the FCC rules in that no

---

<sup>51</sup> This example assumes the company's purpose in collecting such information would be to market, to its customers, services that are outside the category of service to which the customer subscribes. As with the FCC's rules, if the purpose of the list were to enable the company to market additional services in the same category to which the customer already subscribes, no opt-out "approval" would be required. *See section F, infra*.

<sup>52</sup> Our rule for inbound and outbound telemarketing is very similar to the FCC's. Carriers may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call. Because it is oral notice, it requires an express (opt-in) response during the telemarketing call, and as a result a company that uses only private account information in telemarketing will nevertheless have secured opt-in approval for that use.

notice is required for a carrier to use private account information (which is defined to exclude call detail) to market new services within the same category of service to which the customer already subscribes.<sup>53</sup> This allowance is reflected by the white, lower left-hand corner of the box in Table 1, and was present in the prior federal rules, and in our state's rules. We do not, for example, place any restriction on a company's ability to use private account information to market call-waiting services to customers who subscribe to local exchange service but who do not already purchase call-waiting. We find that consumers would not consider it an invasion of their privacy if their own telecommunications provider observes the services they purchase (as distinct from observing, on anything more than a general level, what use they make of those services) and from that observation makes offers of related services. With the added protection our rules afford call detail information, we are confident that a company's use of information about its customers' prior purchases to target its promotion of related services does not upset customers' privacy expectations. Indeed, this is the type of use that is not restricted in other industries, and is typical of a customer-company relationship. We follow the FCC on this point.

## CONCLUSION

105 We have sought to develop rules that are consistent with Section 222 and the FCC's rules interpreting that statute as well as with the U.S. Constitution and our laws and constitution. While we respect the FCC's approach we nonetheless reach a different conclusion on how to harmonize these laws and the interests they protect.<sup>54</sup>

106 We find that the FCC's rules leave certain substantial privacy, speech, and association interests inadequately protected in our state. As the FCC expressly

---

<sup>53</sup> The FCC reasoned that a company's use of CPNI to market services closely related to the those the customer already purchases is an area in which there truly is implied consent on the part of the customer, and that, in section 222 "Congress intended that a carrier could use CPNI without customer approval, but could only do so depending on the service(s) to which the customer subscribes."

<sup>54</sup> Our dissenting colleague has reached a third conclusion—that no CPNI may be disclosed without express consent. We note that his interpretation is even stricter than what was required under our old rules, or under the earlier federal rules, which did not, as the dissent would, require express consent to use CPNI to market even within the same category of services. Also, we feel an obligation to try to harmonize the federal statute with other laws, decisions, and principles, as has the FCC, albeit with a different result. Finally, it is true that the approach Commissioner Hemstad proposes would not be as complex as the one we adopt. Complexity, however, is the price we pay for the complex balancing of the interests at issue.



allowed for in its order, we are adopting rules that are more stringent, in certain respects, than those of the FCC. While our rules follow the framework of the FCC rules, our record supports our adoption of more-stringent protections in three important respects: (1) We provide increased protection for particularly sensitive personal information, including the phone numbers a customer calls and including highly specific phone calling habits of the customer. A company may not use this information, known as “call detail,” without the customer’s express (“opt-in”) approval, except as necessary for the company to provide service or as required by law. (2) We narrow the scope of a telecommunications company’s “family” of affiliated companies, within which it may share information about a customer if the customer does not “opt-out.” The effect is to require express (“opt-in”) approval for disclosure to more types of entities than the federal rules require. (3) We improve the requirements for the notice that companies must provide customers, to help customers understand what is at stake. Also, by requiring companies to offer their customers more convenient methods for opting-out, we enhance customers’ ability to exercise that choice, where applicable.

## ORDER

107 THE COMMISSION ORDERS:

108 WAC sections 480-120-144, 480-120-151, 480-120-152, 480-120-153, 480-120-154 are repealed.

WAC sections 480-120-201, 480-120-203, 480-120-204, 480-120-205, 480-120-206, 480-120-207, 480-120-208, 480-120-209, 480-120-211, 480-120-212, 480-120-213, 480-120-214, 480-120-215, 480-120-216, 480-120-217, 480-120-218, and 480-120-219 are adopted to read as set forth in Appendix C, as rules of the Washington Utilities and Transportation Commission, to take effect pursuant to RCW 34.05.380 (2) on January 1, 2003.

109 This Order and the rule set out below, after being recorded in the register of the Washington Utilities and Transportation Commission, shall be forwarded to the Code Reviser for filing pursuant to chapters 80.01 and 34.05 RCW and chapter 1-21 WAC.

DATED at Olympia, Washington, this 7th day of November, 2002.

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION

MARILYN SHOWALTER, Chairwoman

PATRICK J. OSHIE, Commissioner

Commissioner RICHARD HEMSTAD, dissenting:

- 110 With this Order, my colleagues have done a commendable job of constructing rules that attempt a balance between customer privacy interests and the commercial interests of telecommunications companies. However, the end result is a remarkably complex set of rules which classify customer consent for the use of individually identifiable customer proprietary information in some circumstances by affirmative approval (opt-in), in other circumstances by silence (opt-out), or in still other circumstances by assumed approval with no opportunity even to opt out.
- 111 While these dense rules will be daunting for the affected companies to internalize and implement, they will surely be incomprehensible to even well-informed customers. In contrast, the directive from Congress to this Commission in 47 U.S.C. Sec. 222 is simple and easily understood: Customer approval is required before a telecommunications company may use, disclose or access individually identifiable customer proprietary information except to the extent necessary to operate the public switched telephone network and related activities (e.g., billing). The statute, I believe, can only be fairly read to require the *affirmative* consent of the customer. Consequently, I cannot join in the adoption of these rules concerning customer privacy.

**The constitutionality of 47 U.S.C. § 222 has never been challenged and we cannot act as if it is unconstitutional.**

112 No one has challenged the constitutionality of 47 U.S.C. § 222. It was not challenged in the 10<sup>th</sup> Circuit, and none of the comments we have received have contended it is unconstitutional. A statute is presumed constitutional until it has been determined to be otherwise. We cannot act as if the federal law is unconstitutional and give ourselves permission to invent other ways of treating customer proprietary network information that are inconsistent with the statute. What is adopted today in the sections that do not permit any customer control, and those that permit so-called approval through an opt-out scheme, are, in my opinion, in conflict with the clear, unambiguous grant by Congress to customers of control of the confidentiality of their proprietary network information.

**Congress made a clear statement that individually identifiable customer proprietary network information may not be used without first obtaining approval of the customer.**

113 The language of the statute is unambiguous:

**(c) CONFIDENTIALITY OF CUSTOMER PROPRIETARY NETWORK INFORMATION.—**

**(1) PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS.—**Except as required by law or *with the approval of the customer*, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

47 U.S.C. 222(c)(1) (Italics added).

**Use of customer information without notice to customers and without even the possibility of disapproval is directly contrary to the statute.**

- 114 As stated above, Sec. 222 requires “approval of the customer” before any use, disclosure, or access to individually identifiable customer proprietary network information. The rules adopted today in some circumstances allow telecommunications companies, and any company that controls, is controlled by, or is under common control with a telecommunications company, to use certain customer information *without notice to customers and without their approval*, not even so-called opt out approval. This is an effort, as I understand it, to make the rules acceptable under a *Central Hudson*<sup>55</sup> analysis. Accepting *Central Hudson* as the correct precedent to follow is, in my opinion, a mistake on at least three counts.
- 115 First, *Central Hudson* is a case that did not interpret an explicit federal statutory directive. We should not ignore the fact that Congress has spoken and, in adopting Sec. 222, must be presumed to have weighed the competing values of commercial speech and personal privacy.
- 116 Second, *Central Hudson*’s facts did not involve the use or disclosure of personal information. Rather, it involved an entirely different fact-situation: a utility stuffing, with its monthly bill, a generic advertisement to promote energy consumption in a time of shortage.
- 117 Third, *Central Hudson* addressed only one constitutional issue, the commercial speech rights of a utility to advertise its product free from interference by a regulatory agency. Nothing in the case even remotely touched on what I believe to be constitutionally implicated privacy interests<sup>56</sup> of customers in the confidentiality of their discrete customer information.
- 118 While the FCC may be required to respond to the remand directives of the 10<sup>th</sup> Circuit’s majority opinion,<sup>57</sup> which arrived at its procedural conclusion based upon *Central Hudson*, this Commission is not bound by the 10<sup>th</sup> Circuit’s decision or by its reliance on a case that did not concern a congressional act,

---

<sup>55</sup> *Central Hudson Gas & Elec. Corp. v. Public Service Comm’n of N.Y.*, 447 U.S. 557, 564-65 (1980)(setting out the test to be applied in determining whether restrictions on commercial speech survive “intermediate scrutiny”)

<sup>56</sup> In discussing privacy, I am referencing customers’ rights to privacy, free speech and free association.

<sup>57</sup> The minority opinion, I believe, is the correct view and is true to the language and purpose of Sec. 222.

had completely inapposite facts, and did not address the constitutionally implicated interests that motivated the Commission's departure from the FCC in the first place.<sup>58</sup>

**Approval is not the absence of disapproval, which is all that is represented by opt- out schemes.**

- 119 Other portions of the rules adopted today permit company use of confidential customer information unless the customer opts not to permit such usage. Only the self-interested commenters in this rulemaking promote the view that Congress meant approval to mean the absence of disapproval. It is not a reasonable conclusion; and it is not a conclusion that is permitted in the absence of ambiguity. The proponents of the view that "approval" means an opportunity to opt out rely on wishful thinking, not ambiguity, when they claim it is a reasonable interpretation of the statute.
- 120 Congress constructed a section of law that has as its unmistakable aim the protection of the confidentiality of customer information and it placed the customer in charge of that confidentiality, not telecommunications companies and not regulatory agencies.
- 121 Congress could have been silent on the topic of customer proprietary network information. Then at least an arguable conclusion might be that the information obtained by telecommunications carriers could be treated the same as the information obtained by any other business not the subject of a particular federal statute respecting customer information. Because Congress was not silent, we cannot act as if it were.
- 122 Or, Congress could have constructed a statute like those that are particular to certain activities (e.g., educational and financial institutions, video rental companies) and provided some specific scheme for how the use and disclosure of customer information would be treated. With respect to financial institutions and disclosure of customer information, Congress explicitly used the term "opt out." 15 U.S.C. § 6802(b). When Congress wants to prescribe an opt-out scheme related to customer information, it does so explicitly. But Congress did not prescribe in Sec. 222 the schemes used in other statutes; we

---

<sup>58</sup> Access to information permitted to companies without either customer notice or approval also raises troubling issues of unfair competitive advantage for those companies vis-à-vis their competitors.

cannot act as if it did. Customer information obtained by telecommunications carriers must be treated differently from information obtained by other businesses subject to other, specific statutes adopted by Congress to regulate the use and disclosure of customer information.

123 We can only treat telecommunications customer proprietary information as prescribed in 47 U.S.C. § 222. There is no ambiguity. Congress could have said nothing, or prescribed some other means of safeguarding this information if that is what it had wanted to do. Specifically, it could have created an opt out scheme, but it clearly and unambiguously did not. Instead of silence, an opt out scheme, or something else, it said “with approval of the customer.” A fair reading of the statute compels the conclusion that “approval” can mean only an affirmative statement by a customer, not an assumption of approval based on the absence of disapproval.

**Proponents claim opt out schemes are more efficient and that those who wish to keep their proprietary information private can do so.**

124 If the value sought to be served is efficiency rather than protection of privacy, then proponents probably are correct that use of an opt out scheme would require less effort from telecommunications carriers and only some effort from customers that choose to opt out. However, Congress was in a position to give relative weight to these values—efficiency and personal privacy—and it did so in the language of Sec. 222. It chose efficiency when it did not require customer approval for use of personal information in order to conduct everyday operations of the network, but it also chose to value personal privacy by requiring customer approval of any other use of personal information.

**Washington State policy on privacy is consistent with and reinforces Sec. 222.**

125 Congress has made a determination that telecommunications carriers must protect the confidentiality of customer proprietary network information and must have customer approval to use that information. That is consistent with and reinforced by the strong statement in favor of personal privacy found at Article I, Section 7, of our own Washington Constitution. The adoption of rules that permit use of protected information either without notice or with an opt out scheme is inconsistent with state policy on personal privacy.

### **Concluding Comments.**

- 126 In footnote 54 of the Commission's Order, my colleagues respond to this dissent by asserting that "Complexity...is the price we pay for the complex balancing of interests at issue". But Congress in the unambiguous directive of Sec. 222 did not choose complexity. It chose simplicity. In doing so it mirrored the emphatic views of a broad spectrum of consumers as demonstrated in the enormous outpouring of surprise, anger and distress of Qwest's customers when they became aware of Qwest's intentions to access without their approval what they had assumed to be private information.<sup>59</sup> The Commission's Order, with its complexities, neither responds to these legitimate consumer concerns nor to Sec. 222.
- 127 My colleagues are motivated by considerable concern for customer privacy, which I applaud. That concern is amply demonstrated by their elaborate and scholarly Order. But I nonetheless believe the Commission has followed the wrong case to the wrong result and, in doing so, has ignored the explicit directive of Congress. In an age when huge amounts of personal information can be collected and manipulated, it is my hope that these rules will some day be reviewed by a court that recognizes that the concerns of individuals for their privacy pose new fact-situations that require a fresh analysis. A new precedent for a new environment is in order, one that recognizes the vast changes in technology and its impact on our private lives in the twenty-two years since *Central Hudson*.
- 128 Accordingly, I cannot join in adoption of rules that ignore a customer's statutory right to confidentiality unless the customer gives affirmative approval to a telecommunications company to use, disclose, or access individually identifiable customer proprietary network information.
- 129 For these reasons, I respectfully dissent.

RICHARD HEMSTAD, Commissioner

---

<sup>59</sup> See the description beginning at ¶ 76 of the Order.

*Note: The following is added at Code Reviser request for statistical purposes:*

Number of Sections Adopted in Order to Comply with Federal Statute: New 0, amended 0, repealed 0; Federal Rules or Standards: New 0, amended 0, repealed 0; or Recently Enacted State Statutes: New 0, amended 0, repealed 0.

Number of Sections Adopted at Request of a Nongovernmental Entity: New 14, amended 0, repealed 0.

Number of Sections Adopted on the Agency's own Initiative: New 3, amended 0, repealed 0.

Number of Sections Adopted in Order to Clarify, Streamline, or Reform Agency Procedures: New 0, amended 0, repealed 0.

Number of Sections Adopted using Negotiated Rule Making: New 0, amended 0, repealed 0; Pilot Rule Making: New 0, amended 0, repealed 0; or Other Alternative Rule Making: New 0, amended 0, repealed 0.