Before the
Washington Utilities and Transportation Commission
Olympia, Washington

In Re:	)	Telecommunications - Operations
	)	Chapter 480-120 WAC – Consumer Rules
Telecommunications	)	
Rulemaking	)	Docket No. UT-990146

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

May 22, 2002

Pursuant to the notice and request for public comment published by the Washington Utilities and Transportation Commission (the Commission) on April 5, 2002,[1] requesting comment on the proposed rules concerning telecommunications carriers' use of consumer information, the Electronic Privacy Information Center (EPIC) submits the following comments.

EPIC urges the Commission to protect the privacy rights of American citizens by implementing an opt-in approach towards telecommunications carriers' use of Customer Proprietary Network Information (CPNI), call detail information, subscriber list information, and private account information. Although EPIC believes that an opt-out approach should be used for all these forms of customer information, EPIC supports the opt-in approach the Commission has adopted towards more sensitive forms of customer information.

I. The U.S. West Opinion Does Not Preclude an Opt-in Approach to CPNI Use

In *U.S. West v. FCC*, the 10th Circuit vacated the portion of the Federal Communication Commission's (FCC's) CPNI order and regulations relating to customer opt-in as a violation of the First Amendment. Because the regulations implicated the First Amendment, the court applied the *Central Hudson* commercial speech analysis, which requires the government demonstrate a substantial interest in the speech restriction, and regulations that are narrowly tailored to achieve that interest. The *U.S. West* court assumed that the FCC's stated interests in "protecting customer privacy and fostering competition" were substantial, but found that the CPNI regulations were not narrowly tailored to advance these interests. Specifically, the 10th Circuit criticized the FCC's failure to consider an opt-out approach and to demonstrate that an opt-out approach does not sufficiently protect customer privacy interests. The *U.S. West* court did not hold that an opt-in approach would necessarily violate the First Amendment; it held that the FCC's

[1] Washington Utilities and Transportation Commission, Notice of Opportunity to Comment on Proposed Rule (Apr. 5, 2002).

determination to implement an opt-in approach was not adequately considered or supported by existing facts.

Therefore, in order to implement an opt-in approach for the carriers' use of CPNI in accordance with the First Amendment analysis performed by the *U.S. West* court, the Commission need only demonstrate the following:

(1) That privacy is a substantial government interest; and
(2) There is ample evidence to demonstrate that an opt-out approach is insufficient to protect this interest.

There is substantial available authority to support the above assertions; therefore, employing an opt-in approach is consistent with the First Amendment and is the only reasonable fit with the Commission's intent to protect the privacy of telephone subscribers' personal information.

I. Implementing an Opt-In Approach Satisfies the First Amendment and Serves the Substantial Governmental Interest in Customer Privacy

American jurisprudence recognizes a fundamental right to privacy in personal communications, and the courts and Congress have recognized the paramount interest a citizen has in protecting her privacy.[2] The constitutional right of privacy protects two distinct interests: "one is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[3] Telecommunication carriers' use of sensitive customer information implicates both of these interests.

---

[2] *See, e.g.*, Edenfield v. Fane, 507 U.S. 761, 769 (1993) ("[T]he protection of potential clients' privacy is a substantial state interest."); Sheets v. Salt Lake Cty, 45 F.3d 1383, 1388 (10th Cir. 1995) (where an individual has an expectation that information will not be disclosed, prohibition on such disclosure is a substantial government interest). In Lanphere & Urbaniak v. Colorado, the 10th Circuit recognized that an invasion of privacy is most pernicious when "it is by those whose purpose it is to use the information for pecuniary gain." 21 F.3d 1508, 1511, 1514 (10th Cir. 1994) (applying Central Hudson analysis to uphold a Colorado statute prohibiting public access to criminal justice records "'for the purpose of soliciting business for pecuniary gain'") (quoting Colo. Rev. Stat. § 24-72-305.5 (1992)). This is exactly the purpose for which telecommunications carriers would like to use customer information—to target consumers it believes might be interested in purchasing more of its services.

It is notable also that Congress has recognized the importance of a citizen's privacy interest by enacting statutes preventing disclosure of precisely the same information to the public at large. For example, Congress has enacted an elaborate statutory scheme to protect the privacy of telephone communications, and specifically prohibited the use of pen registers without a court order. 18 U.S.C. §§ 2510-2522 (2002). Thus, Congress has determined that people have a legitimate expectation of privacy with respect to the phone numbers they dial and has decided that this information is so sensitive that it has developed an entire statutory scheme governing law enforcement's ability to collect such data. Similar rules have been established to protect the privacy of cable subscriber records, video rental records, credit reports, and medical records. *See* 18 U.S.C. § 3121 (1994); 47 U.S.C. § 551 (1994); 18 U.S.C. § 2710 (1994); Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994); 42 U.S.C. § 290dd-2(a)(1994); *See generally* Marc Rotenberg, The Privacy Law Sourcebook 2001: United States Law, International Law, and Recent Developments 1- 255 (2001).

[3] Whalen v. Roe, 429 U.S. 589, 599-600 (1977).

Citizens have a legitimate and significant expectation of privacy with respect to sensitive personal information such as which telephone numbers they have dialed. In addition, customers have a right to personally determine how those carriers in possession of their personal information shall use this information.

The fact that some customer information, such as a consumer's name and address, may be publicly available is irrelevant, because "[a]n individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form."[4] Additionally, the protections afforded by the regulations go well beyond concerns with the use or disclosure of publicly available information. The regulations and the underlying statute also protect even more sensitive data about telephone numbers the customer called or from which the customer received a call and the length of the call. As Justice Stewart wrote:

> 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 the places called, and thus reveal the most intimate details of a person's life.[5]

In addition, privacy is a real and significant interest to most Americans: a survey performed in 1999 revealed that the loss of personal privacy was the number one concern of Americans entering the twenty-first century.[6] Numerous polls illustrate public attitudes towards loss of privacy: public trust that commercial institutions will keep confidential data private, while once high, is now tarnished.[7]

II. Opt-In is the Only Truly Effective Means for Protecting the Privacy Interests of Consumers.

The regulations at interest here trigger only intermediate scrutiny under the *Central*

---

[4] Department of Defense v. Federal Labor Relations Auth., 510 U.S. 487, 500-02 (1994) (finding that unions could not use FOIA to obtain the home addresses of federal employees represented by unions).

[5] Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).

[6] Wall Street Journal/NBC News poll, http://www.wsj.com, (Nov. 03, 1999); *see also* Testimony of Lee Rainie before the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce (May 8, 2001) (86 percent of internet users surveyed stated that Internet companies should ask people for permission [opt-in] to use their personal information).

[7] *See* EPIC's Polling Data Page, http://www.epic.org/privacy/survey/default.html; New York Senate Majority Task Force on the Invasion of Privacy, *Public Attitudes about the Privacy of Information*, at http://www.privacyrights.org/ar/invasion.htm at 11-12; Beth Givens, *What's Missing from this Picture? Privacy Protection in the New Millennium*, at http://www.privacyrights.org/ar/naag-mill.htm; Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interests in the 21st Century*, at www.ag.state.mn.us/consumer/Privacy?Default.htm, at 20.

Hudson analysis,[8] under which analysis the means propounded need not be the least restrictive means. Under *Central Hudson*, the government may regulate commercial speech that is neither misleading nor unlawful if: (1) there is substantial interest in support of its regulation; (2) the restriction on commercial speech directly and materially advances that interest; and (3) the regulation is narrowly drawn.[9] The Supreme Court has carefully detailed the difference between the "narrowly tailored" fit required under strict scrutiny, and that required under intermediate scrutiny.

> With respect to this prong, the differences between commercial speech and noncommercial speech are manifest. In *Fox*, we made clear that the "least restrictive means" test has no role in the commercial speech context. "What our decisions require," instead, "is a 'fit' between the legislature's ends and the means chosen to accomplish those ends,' a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is 'in proportion to the interest served,' that employs not necessarily the least restrictive means but … a means narrowly tailored to achieve the desired objective."[10]

Therefore, because the CPNI regulations are subject to intermediate scrutiny, the Commission need not prove that an opt-in regime is the least restrictive alternative, only that it is a "means narrowly tailored to achieve the desired objective."[11]

The Commission's decision to promulgate an opt-in regime for sensitive customer information was the result of careful calculation and assessment of both approaches before the Commission chose to favor the more protective opt-in approach. In addition, there is substantial evidence that opt-out regimes implemented in other circumstances has failed to protect the customer privacy that was the impetus of the regulation.

III. Opt-Out Fails to Protect Customer Privacy

The most glaring inadequacies of an opt-out approach are that (1) the impetus for effective notice rests with entities whose interests are better serviced when there is no effective notice; (2) it assumes a company will, or even can, explain a complex set of legal definitions in a way that will allow for an informed choice.

A. An Opt-Out Approach Does Not Protect Customers From Unwanted Uses of Their Sensitive Personal Information

1. Opt-Out Approach Does Not Provide Notice and Choice to Customers

---

[8] See U.S. West v. FCC, 182 F.3d at 1224, 1232-33 & n.4 (10th Cir. 1999).
http://www.ftc.gov/opa/2001/09/glbwkshop.htm, Sept. 24, 2001 (last accessed Nov. 15, 2001).
[9] Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 564-65 (1980).
[10] Florida Bar v. Went For It, Inc, 515 U.S. 618, 632 (1995).
[11] Id.

An opt-out approach to the use of customer information does not adequately protect a government interest in customer privacy because opt-out systems have systematically failed to give consumers control over their personal information. Therefore, employing an opt-in approach is consistent with the First Amendment and is the only reasonable fit with the intent to protect the privacy of telephone subscribers' personal information.

The danger of the opt-out approach is that because customers may not read their CPNI notices, there is no assurance that any implied consent would be truly informed. Opt-out approaches place an unreasonable burden on telephone customers to take additional steps to protect information that is, by all expectation, confidential. Under the Commission's approach, consumers must give the carrier express approval before the company can divulge their sensitive information such as calling data, which will minimize any unwanted or unknowing disclosure of the information. Under the opt-out approach, consumers may not possess the knowledge that they must affirmatively act to prevent carrier distribution of their information. If they do not have this knowledge, then they cannot exercise discretion regarding it. Therefore, an opt-in approach is the most reasonable fit between the Commission's goal of protecting consumer privacy and the means chosen to reach those ends.

There is substantial independent evidence verifying that an opt-in approach is the only effective method to protect sensitive private information. An opt-out approach is inadequate because it is not calculated to reasonably inform consumers about their privacy options. Not only is the burden on the customer to pay for and return their opt-out notice, such notices are vague, incoherent, and often concealed in a pile of less important notices mailed in the same from the same source.[12] The importance of the notices, as well as their purpose, is rarely brought to the customer's attention in any coherent fashion.[13] Studies have revealed that "the majority of the general public is still unaware of the exact nature of marketing uses and the availability of opt-out choices."[14]

2. Opt-Out Implemented Under Gramm-Leach-Bliley has Proven Ineffective

A true opt-out regime, as implemented under the Gramm-Leach-Bliley Act (GLBA),[15] has generated numerous complaints, as consumers view the financial institutions' unintelligible notices as an attempt to hoodwink them.[16] In fact, the opt-out approach

---

[12] *See* Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* 329-30 (1996) ("The industry itself recommends the use of only vague notices that do not offer meaningful disclosure of practices.")

[13] *Id.*

[14] *Id.* See also Privacy Rights Clearinghouse Second Annual Report 21 (1995), cited in Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1253 n.255 (1998) ("Many consumers are unaware of personal information collection and marketing practices. They are misinformed about the scope of existing privacy law, and generally believe there are far more safeguards than actually exist.")

[15] 15 U.S.C. §§6801-6810 (1999).

[16] *See* Robert O'Harrow Jr., "*Getting a Handle on Privacy's Fine Print: Financial Firms' Policy Notices Aren't Always 'Clear and Conspicuous,' as Law Requires*," WASH. POST, June 17, 2001, at H01.

promulgated under the GLBA has proven so ineffective that the Federal Trade Commission held an Interagency Public Workshop to address some of the concerns raised "about the clarity and effectiveness of some of the privacy notices" sent out by financial institutions in response to the GLBA.[17] In light of the difficulty faced by a federal commission in the implementation of an opt-out approach, it is reasonable for the Commission to have chosen opt-in for sensitive data as a narrowly tailored protection.

The recent experience of consumers with the GLBA further demonstrates the failure of the opt-out regime to adequately protect sensitive personal information. According to the law, financial privacy notices are supposed to be written in a "clear and conspicuous" style; however, few institutions implementing GLB have provided consumers with "clear and conspicuous"[18] notices, as those terms would be defined by most customers. Specifically, the concerns raised by consumers have included complaints that "the notices are confusing and/or misleading and that the opt-out disclosures are hard to find."[19] Opt-out notices mailed out by financial institutions in compliance with the GLBA were unintelligible and couched in language several grade levels above the reading capacity of the majority of Americans.[20] Several experts have highlighted the inadequacy of such statements. Mark Hochhauser, PhD, a readability consultant, reviewed sixty GLBA opt-out notices, calculating that they averaged at a 3rd or 4th year college reading level rather than the junior high level comprehensible to the general public.[21] For example:

> If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law).[22]

Furthermore, individuals can take no comfort in a telecommunications carriers' claim that information is shared only within the "corporate family," or "affiliated parties." Such marketing phrases as "affiliated parties" not only fail to disclose the extent of information-sharing practices but also create a false sense of confidentiality and misplaced trust.

A year of vague, illusive, and unhelpful notices under the GLBA has frustrated and confused consumers while effectively highlighting the fundamental defects of an opt-out regulatory standard.

3. Independent Evidence Verifies that Customers Prefer Opt-In

---

[17] Interagency Public Workshop, "Get Noticed: Effective Financial Privacy Notices," http://www.ftc.gov/bcp/workshops/glb/ (last accessed Apr. 15, 2002); see also Press Release, "Workshop Planned to Discuss Strategies for Providing Effective Financial Privacy Notices," http://www.ftc.gov/opa/2001/09/glbwkshop.htm, Sept. 24, 2001 (last accessed Apr. 15, 2001).
[18] 15 U.S.C. § 6802(b)(1)(A).
[19] *See* Joint Notice Announcing Public Workshop and Requesting Public Comment, "Public Workshop on Financial Privacy Notices," at 3.
[20] *See* O'Harrow, *supra* note 14.
[21] Mark Hochhauser, Ph.D, "Lost in the Fine Print: Readability of Financial Privacy Notices," http://www.privacyrights.org/ar/GLB-Reading.htm, (2001) (last accessed April15, 2002).
[22] *See* Harrow, *supra* note 14.

Choice

Polling data strongly indicates that the American public believes that opt-in is the approach more likely to protect privacy in the deployment of new communications services. According to one nationwide poll released after the *US West* opinion, 86 percent of users of modern communications technologies favor opt-in privacy policies that require explicit customer permission before companies use their personal information.[23] Faced with unintelligible opt-out notices, customers believe that they are purposefully being confused and tricked by the companies sending the notices.[24] Because the Commission intends the proposed rules to protect customer privacy, and the public feels that their privacy is best protected through opt-in regulations, implementation of an opt-in approach would best reflect governmental intent.

Customer opinion about telecommunications carriers use of their personal information was sharply evidenced by the nationwide reaction to opt-out plans implemented by telecommunication carriers in January 2002. In a billing statement sent out in early January 2002, Qwest informed its customers about the calling information collected and marketed by Qwest and gave the customers the option of opting out of the marketing agreement. This notice sparked a public outcry as consumers were taken by surprise that their personal data could be marketed in this manner.[25] Shortly thereafter, SBC Ameritech and Verizon introduced similar marketing plans. In response to violent consumer opposition, Qwest Communications announced that it would withdraw plans for opt-out marketing with CPNI (as defined by 47 U.S.C. § 222).[26] Citing numerous customer concerns, the company stated that it would wait until the FCC's final rulemaking.

The Qwest debacle highlights many of the inadequacies of an opt-out approach, but most particularly illustrates that privacy is an overarching concern to the nation's telecommunications users, and that opt-out notices fail to bring the importance of the decision to the customer's attention.

Company profit underlies all of the arguments in favor of taking control of information away from the consumer. Privacy is a fundamental individual right; companies' interest in profit must be subjugated to protection of this right.

B. Unrestricted Data Sharing Practices Lead to Real Consumer Harms

Identity theft is the fastest growing white-collar crime in America. Identity theft costs over a billion dollars a year, which is then passed on to consumers through higher fees. This does not account for the staggering financial and emotional costs that identity theft

---

[23] *See* Susannah Fox, Trust and Privacy Online: Why Americans Want to Rewrite the Rules, The Pew Internet & American Life Project, Aug. 20, 2000, at 1.
[24] *See* O'Harrow Jr., note 14, supra (quoting Beth Givens, director of Privacy Rights Clearinghouse).
[25] Peter Lewis, *Qwest users upset by opt-out hang-ups*, SEATTLE TIMES, Jan. 08, 2002.
[26] Press Release, Qwest Communications Withdraws Plan to Share Private Customer Account Information Within Company, (Jan 28, 2002) (available at http://www.epic.org/privacy/cpni/qwest_press_release.html)

victims have to bear to clear their good name.[27]

Information-sharing practices of telecommunications carriers increase the risk of identity theft by expanding the number of points where employees or companies might compromise sensitive information.[28] There has been an increase in identity theft cases that occur because dishonest "insiders" are able to gain access to personal information such as the Social Security number.[29] Telecommunications carriers might invest in good security practices and rigorously oversee their employees' work, but they have no control over the practices of third party entities. Furthermore, customers have no means of assessing what might make an affiliated party "trustworthy."

C. Silence Does Not Constitute Customer Approval

Information shared with the consent of the consumer for an identifiable benefit is not a source of public concern. Benefits of information-sharing, such as frequent-flyer programs, would continue to be available under an opt-in system. Customers should be able to make the decision whether actual benefits outweigh the invasion of privacy. What is a source of concern is an example in which a carrier sells private customer information to a third party without a meaningful choice on the part of the consumer.

The proposed rules require a telecommunications carrier to obtain a customer's approval before it can use, disclose, or allow access to that customer's call detail information or other sensitive customer information.[30] Those advocating an opt-out approach rely upon the assumption that customer silence, or inaction, signals approval (permission and intent). This assumption runs counter to all other commercial transactions, in which "approval" requires an affirmative action by an informed consumer.[31] Therefore, the assertion that an opt-out regime is sufficient to assure customer approval (as defined by 47 U.S.C. § 222(c)(1) and incorporated by Proposed Rule WAC 480-120-202) fails to account for the real, legal, and commercial definitions of approval.[32]

---

[27] *See* Linda Foley, Executive Director, Identity Theft Resource Center, Written Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, Identity Theft and Legislative Solutions, (Mar. 20, 2002) available at http://www.idtheftcenter.org/html/s1742.htm; See also "Nowhere to Turn: Victims Speak Out about Identity Theft," by Privacy Rights Clearinghouse and CALPIRG (May 2000), available at http://www.privacyrights.org/ar/idtheft2000.htm.

[28] *See, e.g.*, Marc Rotenberg, Executive Director, EPIC, Written Testimony for Joint Hearing on SSNs and Identity Theft, Subcommittee on Oversight and Investigations, Committee on Financial Services and Subcommittee on Social Security Committee on Ways and Means, U.S. House of Representatives, (Nov. 8, 2001) available at http://www.epic.org/privacy/ssn/testimony_11_08_2001.html.

[29] *See, e.g.*, EPIC's Social Security Number and Privacy Archive, http://www.epic.org/privacy/ssn/.

[30] Proposed Rules WAC 480-120-203 (proposed Apr. 3, 2002).

[31] *See* Jeff Sovern, "Opting in, Opting Out, or No Options at All,: The Fight For Control of Personal Information," 74 WASH. L. REV. 1033, 1105 (1999) ("Normally, silence in commercial settings does not operate as acceptance of an offer. … We do not allow sellers to impose contracts on buyers through negative options, yet we allow sellers to use consumers' personal information as they please without having to give notice."

[32] Black's Law Dictionary defines "approve" as "to give formal sanction to; to confirm authoritatively." BLACK'S LAW DICTIONARY 98 (7th ed. 1999). Webster's defines "approval" as " formal consent or sanction," while sanction is defined as "*to grant permission*." WEBSTER'S NEW WORLD DICTIONARY 68, 302 (2nd College Ed. 1984). Commercial contracts require the party to the contract to give affirmative

An opt-out system at its very heart carries the assumption that there will be little response to the notices because the notices will be overlooked, or will be too complicated to understand. Like other negative choice systems, permission though silence will invariably get a large percentage of "yes" responses because no response is necessary. Telecommunications carriers often assert that the low percentage of opt-out rates indicate that customers do not in fact value the privacy of their personal information. Expert studies illustrate that, in fact, few consumers recall seeing notices even when the notices are required to be clear and conspicuous, which suggests that when businesses do not want consumers to see a notice, consumers will not.[33] Furthermore, companies are versant in how to best phrase and send opt-out notices to maximize customer confusion, and to minimize the chance that customers will read the notices.[34] In addition, companies know how to send out their opt-out notices in a manner least likely to be noticed, opened, or read by customers.[35] This unfairly places the burden on the individual who is concerned about protecting privacy and not where the burden belongs – on the company that will profit from use of the personal information.

An opt-in scheme would completely reverse this by making it in a company's best interest to explain its information-sharing practices in a way that individuals can understand and accept. This step is necessary to ensure that customers have knowledgeably consented to use of their personal information, and have not been tricked or confused into assenting to the loss of something they valued.

D. An Opt-In System Improves Information Flow, Increases Quality of the Telecommunications Service, and Reduces Prices

Proponents of an opt-out approach argue that such a system is economically preferable, as it increases the amount of information available to both producers and consumers, allows telecommunications carriers to improve services offered by tailoring these services to specific customers, and reduces prices. This assertion erroneously assumes that the only costs at issue are those of production, without accounting for increased transaction costs incurred by the consumer in seeking to exercise privacy rights created by statute.[36]

Opt-out regimes create an economic incentive for businesses to make it difficult for consumers to exercise their preference not to disclose personal information to others. Because opt-out systems do not require businesses to create inducements for consumers to choose affirmatively to disclose personal information, these systems encourage firms to engage in strategic behavior and thus inflate consumer transaction costs.[37] In contrast,

---

approval before the contract is considered valid. Richard A. Lord, A Treatise on the Law of Contracts 6:3, 6:49, at 17-18, 561 (14th ed. 1991).

[33] Sovern, *supra* note 31, at 1099.

[34] *See* Ting v. AT&T No. C 01-02969 BZ, ¶33 (Jan. 15, 2002)

[35] *See id*. at ¶¶25-28.

[36] *See* Sovern, supra note 31, at 1082-83.

[37] *See id*. at 1099-1100.

an opt-in system would permit consumers who wish to protect their privacy to do so, while encouraging telecommunications carriers to eliminate consumer transaction costs.[38] Because carriers profit from the use of consumer information, and thus want as much information as possible, carriers would have an incentive to make it as easy as possible for consumers to consent to the use of their personal information. Such a system might include a comprehensible list of the benefits to opting-in, contained within a clearly marked mailing, with a pre-paid stamped envelope. This would preclude the transaction costs involved with attempting to contact via phone customers with the authority to opt-in. It also reduces the strategic behavior costs associated with opt-out—the costs associated with providing consumers a message that they don't want consumers to receive—because the telecommunications carriers would have an incentive to lower costs associated with providing customers a message that they are very eager to have the customer receive.[39] Finally, opt-in may decrease the amount of information in the marketplace, but it permits telecommunications carriers to target products at those who have specified an interest in such information: thereby decreasing the wasted costs associated with targeting uninterested customers.[40]

IV. Legal Scholars Believe Opt-In is Both Fair and Efficient

Legal scholars who have considered the issue of opt-in versus opt-out have invariably concluded that the opt-in regime is both more likely to safeguard privacy interests and is more economically efficient. Opt-in upholds the primary purpose of privacy legislation: to ensure that consumers are given some effective means of control over the use of personal information held by others. As Professor Mark Budnitz explained:

> Consumers should have the ability to opt in because a choice to opt in gives consumers, in the first instance, greater control over their personal information. . . . Consumers may fail to opt out for a variety of reasons that have little to do with whether they truly want a company to collect and disseminate information about them. For example, they may not understand the nature of the information that will be collected, aggregated, and disseminated; how the company will use the information for its internal purposes; the nature of third parties to whom the data may be distributed; or what those third parties may do with the data. . . . Moreover, the opt-out method is easy for companies to abuse. The opt-in approach is far more consistent with consumer control because it assumes consumers do not want their privacy invaded. Therefore, consumers automatically are protected from invasions. If consumers are willing to give away their privacy or to trade it in return for a benefit they desire, they have the ability to do so.[41]

---

[38] *See id.*

[39] *See id*. at 1101-02.

[40] *See id*. at 1103.

[41] Mark E. Budnitz, "Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate," 49 S.C. L. REV. 847 (1998).

In the specific context of CPNI, legal scholars have determined that the opt-in rule promotes markets efficiency. As Professor Paul Schwartz has observed:

> The goal regarding individually identified CPNI should be to find a way to permit consumers to make informed decisions about use of their information at the least cost to them. To reach this goal, companies should be forced to internalize not only their own costs but at least some of their customers'. Such action, by raising the "price" of personal information and privacy violations, will improve efficiency in "privacy price discrimination."[42]

Professor Julie Cohen's review of the nature of consent obtained under the two regimes emphasizes the significance of opt-in as the more efficient way to allocate the burden to act where information asymmetries exist:

> If we reconceptualized the government interest in protecting data privacy as an interest in correcting information asymmetries in the market for personally-identified data, the Central Hudson analysis (or a more stringent review) might proceed quite differently. In particular, an explicitly economic approach to regulation of speech markets would save regulations like the opt-in rule challenged in U.S. West, which focus on the quality as well as the fact of consent.[43]

Professor Daniel Solove, reviewing this recent literature on opt-in versus opt-out regimes, writes:

> Thus, providing people with opt-out rights and privacy policies does little to give individuals much control over the information collected and used. Regulation mandating that consumers opt-in rather than opt-out will more effectively control the flow of information between unequal parties.[44]

Professor Solove concludes, "effective privacy regulation must require an opt-in system which requires a meaningful range of choices as well as addresses inequalities in knowledge and power and other impediments to voluntary and informed consent."[45]

V. Conclusion

There is a longstanding historical, legal, and legislative record providing that protection of privacy is a real, substantial, and significant concern. The Commission will protect the

---

[42] Paul M. Schwartz, "Charting a Privacy Research Agenda: Responses, Agreements, and Reflections," 32 CONN. L. REV. 929, 936 (2000)

[43] Julie E. Cohen, "Examined Lives: Informational Privacy and the Subject as Object," 52 STAN. L. REV. 1373, 1414 (May 2000).

[44] Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," 53 STAN. L. REV. 1393 (July 2001).

[45] *Id.* (emphasis added).

privacy interests of those using the Nation's telecommunications system by enacting an opt-in approach towards telecommunications carriers' use of customer information. A customer has a reasonable expectation that her personal information will be kept private. Customers provide information to their telecommunication carriers with the expectation that the information will be kept confidential, and have no viable alternative regarding their carrier's collection of information. Although customers are aware that this information is captured by the telecommunication carrier in providing a necessary service, this initial capture does not provide the right of further dissemination of private information. An opt-in approach to sensitive information not only protects the privacy interests of telephone customers, but also preserves important values recognized in the First Amendment context, which is the right of telephone customers to decide, freely and without unnecessary burden, when they wish to disclose personal information to others.[46] The ability of individuals to keep private the records of their personal communications also serves the constitutional interest in not chilling communications between free individuals through the fear of private surveillance.[47]

The *U.S. West* court vacated the FCC opt-in rulemaking because there was no showing of specific harm that would result to customers upon implementation of the less speech-restrictive opt-out approach. These comments illustrate that there is ample evidence of such harm that has resulted to consumers upon implementation of similar systems. In the light of such tangible evidence, the Commission's interest in protecting the privacy of telecommunications customers can only be met by implementing an opt-in approach towards sensitive customer information.

EPIC respectfully urges the Commission to promulgate the proposed opt-in standard for the disclosure of customer information. Although EPIC believes that these comments provide support for a regulation implementing an opt-in approach towards all customer information—including CPNI—EPIC applauds the Commission's efforts to restrict use of more sensitive forms of customer information.

Respectfully submitted,

Mikal J. Condon, esq., Staff Counsel
Electronic Privacy Information Center
1718 Connecticut Ave., NW Suite 200
Washington, DC 20008
1 202 483 1140 (tel)
1 202 483 1248 (fax)
May 22, 2002

---

[46] *See generally* Buckley v. American Constitutional Law Found., Inc., 525 U.S. 182 (1999); McIntyre v. Ohio Elections Comm'n,514 U.S. 334 (1995); Talley v. California, 362 U.S. 60 (1960).
[47] *See* NAACP v. Alabama, 357 U.S. 449, 462 (1958); see also Smith v. Maryland, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting).