Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	**)**	
	)	
Telecommunications Carriers'	**)**	**CC Docket No. 96-115**
Use Of Customer	**)**	**CC Docket No. 96-149**
Proprietary Network Information	**)**	

To: The Commission

COMMENTS OF
THE ELECTRONIC PRIVACY INFORMATION CENTER, AMERICAN CIVIL LIBERTIES UNION, AMERICAN LIBRARY ASSOCIATION, CENTER FOR DIGITAL DEMOCRACY, CENTER FOR MEDIA EDUCATION, COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY, CONSUMER ACTION, CONSUMER FEDERATION OF AMERICA, JUNKBUSTERS, MEDIA ACCESS PROJECT, NATIONAL CONSUMERS LEAGUE, NETACTION, PRIVACYACTIVISM, PRIVACY JOURNAL, PRIVACY RIGHTS CLEARINGHOUSE, PRIVACY TIMES, PUBLIC CITIZEN LITIGATION GROUP, AND US PIRG

November 1, 2001

Pursuant to the notice published by the Federal Communications Commission on October 2, 2001 regarding Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, the Electronic Privacy Information Center American Civil Liberties Union, American Library Association, Center for Digital Democracy, Center for Media Education, Computer Professionals for Social Responsibility, Consumer Action, Consumer Federation of America, Junkbusters, Media Access Project, National Consumers League, NetAction, Privacyactivism, Privacy Journal, Privacy Rights Clearinghouse, Privacy Times, Public Citizen Litigation Group, and US PIRG submit the following comments.

The Commentators urge 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) pursuant to section 222 of the Communications Act of 1996. The Commission has a fundamental responsibility, mandated by Congress in the passage of the Communications Act of 1996, to protect the privacy interests of those using the Nation's telecommunications system. This responsibility can only be met by adopting an opt-in approach to the use of customer CPNI by telephone companies.

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 Commission's CPNI order and regulations relating to customer opt-in as a violation of the First Amendment.[1] 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.[2] The *U.S. West* court assumed that the Commission's stated interests in "protecting customer privacy and fostering competition" were substantial,[3] but found that the CPNI regulations were not narrowly tailored to advance these interests. Specifically, the 10th Circuit criticized the Commission'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 Commission's determination to implement an opt-in approach was not adequately considered or supported by existing facts.[4]

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 underlying the adoption of 47 U.S.C. 222; 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 Congressional intent to protect the privacy of telephone subscribers' personal information.

II. Privacy is a Substantial Government Interest Underlying the Enactment of Section 222

A. Congressional Intent Underlying Section 222 was to Protect Customer Privacy

When Congress enacted section 702 of the Telecommunications Act of 1996, its express intent was to protect the privacy interests of consumers by insisting that confidential information remain protected. Section 702 of the Telecommunications Act of 1996 requires all telecommunications carriers "to protect the confidentiality of proprietary

[1] 182 F.3d at 1224, 1240 (10th Cir. 1999).
[2] *Id.* at 1233-34 (citing Central Hudson Gas and Elec. Corp. v. Public Service Commission, 447 U.S. 557 (1980))
[3] The U.S. West court declined to find that promoting competition was a substantial interest behind the Congressional adoption of Section 222 because the section makes no mention of competition; however, determined that Congress "may not have completely ignored competition in drafting 222." Id. at 1235-37.
[4] Id. at 1238-40. ("The dissent accuses us of 'advocating' an opt-out approach. We do not 'advocate' any specific approach. We merely find fault in the FCC's inadequate consideration of the approval mechanism alternatives in light of the First Amendment.")

information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."[5] Specifically, a telecommunications carrier is precluded from disclosing CPNI it receives as a result of providing its service without customer approval, subject to narrow exceptions.[6]

Section § 222(c)(1) requires a telecommunications carrier to obtain a customer's *approval* before it can use, disclose, or allow access to that customer's CPNI.[7] In its report on the legislation that was eventually enacted as the Telecommunications Act of 1996, the House Commerce Committee explained that the purpose of the protections contained in this section was to balance "the need for customers to be sure that personal information that carriers may collect is not misused" against the customer's interest in ensuring "that when they are dealing with their carrier concerning their telecommunications services, the carrier's employees will have available all relevant information about their service."[8]

B. The Supreme Court has Recognized that an Interest in Privacy of Personal Information is Substantial

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.[9] 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."[10] Telecommunication carriers' use of CPNI implicates both of these interests. 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 CPNI, 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

---

[5] Telecommunications Act of 1996 § 702(a), 47 U.S.C. § 222(a) (Supp. III 1997).
[6] See id
[7] See id.
[8] H.R. Rep. No. 104- 204, pt. 1, at 90 (1995).
[9] 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 U S West would like to use CPNI—to target consumers it believes might be interested in purchasing more of its services.
[10] Whalen v. Roe, 429 U.S. 589, 599-600 (1977).

information may be available to the public in some form."[11] 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.[12]

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.[13]

It is notable that Congress recognized the importance of a citizen's privacy interest by enacting other 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,[14] and specifically prohibited the use of pen registers without a court order.[15] 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,[16] video rental records,[17] credit reports,[18] and medical records.[19]

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

A. FCC Rejected an Opt-Out Approach as Inadequate After Careful Consideration and Debate.

---

[11] 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).
[12] Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).
[13] 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).
[14] See 18 U.S.C. §§ 2510-2522 (1994 & Supp. III 1997).
[15] See 18 U.S.C. § 3121 (1994).
[16] See 47 U.S.C. § 551 (1994).
[17] See 18 U.S.C. § 2710 (1994).
[18] See Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994).
[19] See 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).

When the Commission originally contemplated its order, it considered the feasibility of adopting an opt-out approach, and carefully calculated the risks and benefits of this approach before rejecting it in favor of a more protective opt-in approach.[20] As the Commission explained, 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."[21] The Commission did not casually or arbitrarily select the opt-in over the opt-out approach; instead, the Commission read Section 222, solicited and studied comments from all interested parties, and carefully chose the option it believed best represented the intent of Congress and best protected the privacy rights of customers. Moreover, the alternative opt-out approach that was rejected by the Commission would have placed an unreasonable burden on telephone customers to take additional steps to protect information that is, by all expectation, confidential.

Under an opt-in approach, consumers must give the carrier express approval before the company can divulge their CPNI, which, as the Commission explained, "will minimize any unwanted or unknowing disclosure" of the information.[22] Under the opt-out approach, consumers may not possess the knowledge that they must affirmatively act to prevent carrier distribution of their CPNI. If they do not have this knowledge, then they cannot exercise discretion regarding it. Because "approval" requires an affirmative action by an informed consumer, only the opt-in approach satisfies congressional intent. It is the most reasonable fit between Congress's ends and the means chosen to reach those ends.

B. Independent Evidence Corroborates that Opt-Out Fails to Protect Customer Privacy

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.[23] The importance of the notices, as well as their purpose, is rarely brought to the customer's attention in any coherent fashion. 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."[24] Opt-out notices mailed out by financial institutions in compliance with the Gramm-

[20] See CPNI Order at 20,327-20,338.
[21] See id.
[22] Id. at 329.
[23] 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.")
[24] 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.")

Leach-Bliley Act (GLBA) were unintelligible and couched in language several grade levels above the reading capacity of the majority of Americans.[25]

The common-sense definition of "approval," the key term in the statute, weighs heavily in favor of the view of the 15 consumer and privacy organizations submitting these comments that opt-in is necessary to protect consumer privacy interests. Black's Law Dictionary defines "approval" as "[t]he act of confirming, ratifying, assenting, sanctioning, or consenting to some act or thing done by another. 'Approval' implies knowledge and exercise of direction after knowledge. Id. at 102 (6th ed. 1990). The opt-out approach fails to satisfy the definition of approval because the customer is not confirming or ratifying anything. Under the opt-out approach, consumers may not possess the knowledge that they must affirmatively act to prevent carrier distribution of their CPNI. If they do not have the knowledge, then they cannot exercise discretion regarding it.

In addition, 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.[26] Faced with unintelligible opt-out notices, customers believe that they are purposefully being confused and tricked by the companies sending the notices.[27] Because Congress intended section 222 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 congressional intent.

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

There is a longstanding historical, legal, and legislative record providing that protection of privacy is a real, substantial, and significant concern. In addition, there is a specific legislative record detailing that this concern was a primary impetus behind the congressional enactment of Section 222. The Commission will uphold congressional intent to protect the privacy interests of those using the Nation's telecommunications system by enacting an opt-in approach towards telecommunications carriers' use of customer proprietary network information (CPNI). 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

[25] The GLBA requires banks, insurance agencies, and brokerage firms to send notice and opportunity to opt-out to customers before sharing their non-public information. 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," Washington Post, June 17, 2001, at H1. O'Harrow's article cites language specialist Hochhauser, who stated that a reader would have to be reading at a 3rd or 4th year college level in order to decipher the privacy notices, while most Americans read at a junior high school level. Id.

[26] 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.

[27] See O'Harrow Jr., note 25, supra (quoting Beth Givens, director of Privacy Rights Clearinghouse).

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 CPNI use 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.[28] 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.[29] On behalf of millions of telephone customers in the United States, the Commentators respectfully urge the Commission to adopt an opt-in standard for the disclosure of customer CPNI.

Respectfully submitted,

Marc Rotenberg, esq., Executive Director
Mikal 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)

November 1, 2001

[28] 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).
[29] See NAACP v. Alabama, 357 U.S. 449, 462 (1958); see also Smith v. Maryland, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting).