Before the
Federal Communications Commission
Washington, DC 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 ATTORNEYS GENERAL OF ALASKA, ARIZONA, ARKANSAS, CALIFORNIA, COLORADO, CONNECTICUT, FLORIDA, HAWAII, IDAHO, IOWA, KANSAS, MAINE, MARYLAND, MASSACHUSETTS, MICHIGAN, MINNESOTA, MISSISSIPPI, MISSOURI, NEVADA, NEW HAMPSHIRE, NEW JERSEY, NEW MEXICO, NEW YORK, NORTH CAROLINA, OHIO, OKLAHOMA, OREGON, PENNSYLVANIA, RHODE ISLAND, SOUTH CAROLINA, SOUTH DAKOTA, TENNESSEE, TEXAS, VERMONT, WASHINGTON, WEST VIRGINIA, WISCONSIN, WYOMING, THE TERRITORY OF THE U.S. VIRGIN ISLANDS, THE DISTRICT OF COLUMBIA'S CORPORATION COUNSEL, AND THE ADMINISTRATOR OF THE GEORGIA GOVERNOR'S OFFICE OF CONSUMER AFFAIRS

December 21, 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, we the undersigned Attorneys General submit the following comments.

The States urge the Commission to protect the privacy rights of consumers by implementing an opt-in approach towards telecommunications carriers' use of Customer Proprietary Network Information ("CPNI") pursuant to § 222 of the Telecommunications Act of 1996 ("the Act"). In the Act, Congress mandates that the Commission protect the privacy interests of consumers who use the telecommunications system. The FCC can meet this responsibility, and satisfy its constitutional duty to adopt a narrowly tailored regulatory scheme, only by adopting an opt-in approach to use of customer CPNI by telephone companies.

I. Background: The Commission May Use An Opt-In Approach After Building An Appropriate Record.

47 U.S.C. § 222, enacted as part of the Telecommunications Act of 1996, states generally that every telecommunications carrier has a duty to protect the confidentiality of proprietary information relating to consumers, and places restrictions on carriers' use, disclosure of and access to certain customer information to effectuate that duty. The statute recognizes three types of customer information: (1) CPNI; (2) aggregate customer information; and (3) subscriber list information.

The technical definition of CPNI is contained in 47 U.S.C. § 222(h)(1)(A)-(B); in sum, CPNI amounts to when, where, and to whom a customer places calls.[1] "Given the sensitive nature of some CPNI, ..., Congress afforded CPNI the highest level of privacy protection under § 222." *U.S. West, Inc. v. F.C.C.*, 182 F.3d. 1224, 1228-29, n.1 (10th Cir. 1999).

The critical provision of § 222 dealing with CPNI is subsection (c)(1), which the FCC has found limits a carrier's use of CPNI to marketing within the consumer's chosen class of service, "[e]xcept as required by law or with the *approval* of the customer".[2] Thus, "the essence of the statutory scheme [governing use of CPNI] requires a telecommunications carrier to obtain customer approval when it wishes to use, disclose, or permit access to CPNI in a manner not specifically allowed under § 222." 182 F.3d at 1229.

In light of numerous questions by the industry with respect to what type of "approval" was necessary under the statute, the Commission adopted regulations in 1998 that interpreted § 222's consumer approval requirements. In construing the dictates of § 222, the FCC regulations permit a carrier to use, disclose, or share CPNI without customer approval for the purpose of marketing products within a

---

[1] However, some States, such as Minnesota, have construed the definition of CPNI more broadly to include unlisted and unpublished telephone numbers.

[2] "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." See 47 U.S.C. § 222(c)(1).

category of service to customers, provided the customer already subscribes to that category of service.[3] Also in construing the dictates of § 222, the FCC regulations prevent use of CPNI without customer approval for (1) marketing customer premises equipment or information services (such as call answering, voice mail, or Internet access services); (2) identifying or tracking customers who call competitors; or (3) attempting to regain customers who have switched to another carrier. See 47 C.F.R. § 64.2005(b)(1)-(2).

The regulations set forth the means by which a carrier must obtain consumer "approval." The Commission determined that the Act's "approval" requirement dictated an opt-in approach, in which a carrier must obtain prior express approval of a customer through written, oral, or electronic means before using the customer's CPNI. 47 C.F.R. § 64.2007(a) & (b).

U.S. West, Inc., challenged under the First Amendment the Commission's regulations implementing the CPNI privacy provisions of § 222 of the Act.[4] In *U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224 (10th Cir. 1999), the Tenth Circuit, employing the Supreme Court's *Central Hudson*[5] test for permissible regulation of commercial speech, vacated the portion of the Commission's CPNI order and regulations that required customer opt-in before carriers could use the information outside one of the statutory exceptions. 182 F.3d at 1240. While the Tenth Circuit assumed that the Commission's stated interest for its opt-in rule – protecting consumer privacy – was substantial, the court found that the record did not demonstrate that the opt-in approach appropriately advanced this interest. *Id.* at 1238-40. Specifically, the court held that the record failed to demonstrate that (1) the CPNI regulations directly and materially advance the Commission's interest in protecting consumers' privacy, and (2) that the opt-in mechanism for ensuring consumer "approval" of use of CPNI was narrowly tailored. *Id.* at 1237-39. The Tenth Circuit did not hold that an opt-in approach would necessarily violate the First Amendment, nor that an opt-out approach was the only mechanism available that satisfied the requirements of the Constitution:

[3] The categories of service at issue were: (1) local; (2) interexchange, which includes most long-distance service; and (3) commercial mobile radio service, which includes mobile and cellular service.

[4] U.S. West also challenged the CPNI regulations under the Fifth Amendment, as an unconstitutional taking, but in light of its First Amendment ruling the court did not reach the Fifth Amendment issue.

[5] *Central Hudson Gas and Elec. Corp. v. Public Service Commission*, 447 U.S. 557 (1980).

> 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.

Id. at 1240, n.15.

In its October 2, 2001, request for comments, the Commission has asked the public to comment upon the type of consumer "approval" that it should require before carriers can share CPNI in light of the *U.S. West* decision. The States suggest that, in reexamining the rules that appropriately should govern selling or sharing of CPNI, the Commission should focus upon the following two inquiries:

> (1) Whether the regulation of CPNI directly and materially advances the Commission's interest in protecting consumers' privacy; and
>
> (2) Whether there is ample evidence to demonstrate that an opt-in approach is narrowly tailored.

The States believe that the Commission should answer both these inquiries in the affirmative.

II. The Requirement of Customer Approval Prior to Use of CPNI Directly and Materially Advances the Commission's Interest in Privacy.

The CPNI rules seek to address the harm to a consumer resulting from disclosure of his or her CPNI information – when, where and to whom the customer places calls – without a customer's consent. This is precisely the type of information that is among the most sensitive and worthy of protection:

> 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.[6]

The States believe that in the absence of § 222 of the Act, and the Commission's implementing regulations, it is clear that carriers would disclose CPNI for purposes unrelated to the customer's current telecommunication services. 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

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

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 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.

These scenarios do not amount to mere speculation. In the financial services sector, industry members have long been sharing with joint marketers and third parties such sensitive information as credit card accounts, balances, and purchases made. In the spring of 1999, the Minnesota Attorney General announced a settlement with U.S. Bank resolving allegations that the Bank misrepresented its practice of selling highly personal and confidential financial information regarding its customers to telemarketers. One year later, thirty-nine additional states and the District of Columbia entered into a similar settlement.[7] The multi-state investigation focused on the bank's sale of customer information, including names, addresses, telephone numbers, account numbers and other sensitive financial data, to marketers. The marketers then made telemarketing calls and sent mail solicitations to the bank's customers in an effort to get them to buy the marketers' products and services, including dental and health coverage, travel benefits, credit card protection, and a variety of discount membership programs. Buyers were billed for these products and services by charges placed on their U.S. Bank credit card. In return for

[7] The basis for the states' action was their charge that U.S. Bank misrepresented its privacy policy to its customers. In some account agreements provided to its customers, the bank listed the circumstances under which information would be disclosed, but failed to include any reference to the bank's practice of providing such information to vendors for direct marketing purposes. In other instances, the bank had specifically represented that customer information would be kept confidential.

providing confidential information about its customers, U.S. Bank received a commission of 22 percent of net revenue on sales with a guaranteed minimum payment of $3.75 million.

Subsequent to the U.S. Bank case, and as a result of heavy lobbying by industry, Congress authorized financial services companies to sell or give their customers' nonpublic personal information to both joint marketers and third party telemarketers. The extent to which consumers actually "approve" of this sharing of nonpublic personal information about them is discussed below. For purposes of discerning whether the harm addressed by the CPNI rule is "real," it is fair to say that consumers' experiences in the financial services sector demonstrate that, despite the competitive nature of the information at issue, carriers will find irresistible the opportunity to sell or share CPNI with marketing partners or third party telemarketers.

III. Use of An Opt-In As The Mechanism to Obtain Customer Approval Is Sufficiently Narrowly Tailored.

As noted above, § 222 of the Act requires that carriers obtain customer "approval" prior to using, disclosing, or permitting access to personally identifiable CPNI, except in certain limited circumstances. Congress did not define this key term in the statute. The States believe that this term must be given its ordinary and natural meaning. 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 discretion after knowledge." BLACK'S LAW DICTIONARY 102 (6th ed. 1990).

The opt-out approach does not satisfy the requirement of "knowledge and exercise of discretion after knowledge," because notices provided by the carriers will not be sufficient to give consumers the knowledge they need about the nature of the information being shared or sold, the circumstances under which the information will be shared or sold, and the effect or result of the sharing or selling of the information. Because consumers may not have knowledge about the information sharing at issue, they would not have the ability to exercise discretion with respect to that knowledge.

When the Commission originally contemplated regulations under § 222 of the Act, it considered the feasibility of adopting an opt-out approach. After carefully calculating the risks and benefits of this approach, the Commission rejected the opt-out approach in favor of the more protective opt-in approach. *See* 63 Fed. Reg. 20,326, 20,327-38. The Commission concluded that an express approval mechanism will ensure an informed and deliberate response, while an opt-out approach would be inadequate under the statutory scheme, because consumers may not receive or read their CPNI notices, and they may not understand that they must take affirmative steps to protect access to their sensitive information. The Commission therefore concluded that there would be no assurance that implied consent from consumer inaction would be truly informed. *Id*.

The Commission was correct in its selection of the opt-in mechanism to ensure compliance with the statutory requirement of customer "approval." Experience with opt-out notices under Gramm-Leach-

Bliley demonstrates that consumers' inaction does not indicate "knowledge and exercise of discretion after knowledge." The Gramm-Leach-Bliley Act requires banks, insurance agencies, and brokerage firms to send notice and opportunity to opt-out to customers before sharing their non-public information with certain entities.[8]

According to GLB, these financial privacy notices are supposed to be written in a "clear and conspicuous"[9] manner; however, the opt-out notices provided to consumers by many institutions implementing GLB have not been "clear and conspicuous," as those terms are commonly understood. Opt-out notices mailed by many financial institutions have been unintelligible and couched in language several grade levels above the reading capacity of the majority of Americans.[10] Experts have highlighted the inadequacy of such statements. Mark Hochhauser, Ph.D., a readability expert, reviewed sixty GLB Act opt-out notices. Dr. Hochhauser determined that these notices were written at an average 3d or 4th year college reading level, rather than the junior high level comprehensible to the general public.[11] For example, the notice sent to customers by one financial institution stated:

> 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).[12]

Recent surveys demonstrate that consumers either never see and read such complicated opt-out notices, or they don't understand them. A survey conducted by the American Bankers Association[13] found that 41% of consumers did not recall receiving their opt-out notices, 22% recalled receiving them but did not read them, and only 36% reported reading the notice. Another survey, conducted by Harris Interactive for the Privacy Leadership Initiative, announced its results in early December 2001.[14] The Harris survey indicated that only 12% of consumers carefully read GLB privacy notices most of the time,

---

[8] *See* 15 U.S.C. §§ 6801-6809 (1999).
[9] *Id*. at § 6802(b)(1)(A).
[10] *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*, The Washington Post, June 17, 2001, at H-01.
[11] Mark Hochhauser, Ph.D., "Lost in the Fine Print: Readability of Financial Privacy Notices," http://www.privacyrights.org/ar/GLB-Reading.htm (2001).
[12] *See* O'Harrow, *supra* n.9.
[13] Available at http://www.aba.com/Press+Room/bankfee060701.htm
[14] Available at http://www.ftc.gov/bcp/workshops/glb.

whereas 58% did not read the notices at all or only glanced at them. The Harris survey further indicated that lack of time or interest *and* difficulty in understanding or reading the notices top the list of the reasons why consumers do not spend more time reading them.

Where the vast majority of consumers don't even read opt-out notices, it cannot be said that they "approve" the sharing or selling of their personal nonpublic information.

Those consumers that do read the GLB notices have voiced numerous complaints, raising concerns that the financial institutions' unintelligible notices are an attempt to mislead them.[15] The opt-out approach promulgated under GLB has proven so problematic that the federal agencies that administer the regulations under GLB convened an Interagency Public Workshop to address the concerns that have been raised "about clarity and effectiveness of some of the privacy notices" sent out under GLB.[16] The agencies note that consumers have complained that "the notices are confusing and/or misleading and that the opt-out disclosures are hard to find."[17]

The difficulty faced by consumers of financial services under GLB's opt-out regime militates strongly in favor of adoption by the Commission of an opt-in approach to demonstrate consumer "approval" of use of CPNI. Only opt-in ensures that consumers have received and read the notice and made an affirmative decision to allow their personal information to be shared.

---

[15] *Id*.

[16] Interagency Pubic Workshop, "Get Noticed: Effective Financial Privacy Notices", http://www.ftc.gov/bcp/workshops/glb/ ; 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).

[17] See Joint Notice Announcing Public Workshop and Requesting Public Comment, "Public Workshop on Financial Privacy Notices," at 3.

IV. Conclusion

The States urge the Commission to require carriers to seek consumer approval through an "opt in" approach prior to allowing the carriers to share personal calling data collected as CPNI. The States thank the Commission for considering the views of the States.

Bruce M. Botelho
Attorney General of Alaska

Janet Napolitano
Attorney General of Arizona

Mark Pryor
Attorney General of Arkansas

Bill Lockyer
Attorney General of California

Ken Salazar
Attorney General of Colorado

Richard Blumenthal
Attorney General of Connecticut

Robert R. Rigsby
Corporation Counsel of the
District of Columbia

Robert A. Butterworth
Attorney General of Florida

Barry W. Reid
Administrator of the Georgia
Governor's Office of Consumer Affairs

Earl Anzai
Attorney General of Hawaii

Alan G. Lance
Attorney General of Idaho

Tom Miller
Attorney General of Iowa

Carla J. Stovall
Attorney General of Kansas

G. Steven Rowe
Attorney General of Maine

J. Joseph Curran, Jr.
Attorney General of Maryland

Tom Reilly
Attorney General of Massachusetts

Jennifer Granholm
Attorney General of Michigan

Mike Hatch
Attorney General of Minnesota

Mike Moore
Attorney General of Mississippi

Jeremiah W. Nixon
Attorney General of Missouri

Frankie Sue Del Papa
Attorney General of Nevada

Philip T. McLaughlin
Attorney General of New Hampshire

John J. Farmer, Jr.
Attorney General of New Jersey

Patricia Madrid
Attorney General of New Mexico

Eliot Spitzer
Attorney General of New York

Roy Cooper
Attorney General of North Carolina

Betty D. Montgomery
Attorney General of Ohio

W. A. Drew Edmondson
Attorney General of Oklahoma

Hardy Myers
Attorney General of Oregon

D. Michael Fisher
Attorney General of Pennsylvania

Sheldon Whitehouse
Attorney General of Rhode Island

Charlie Condon
Attorney General of South Carolina

Mark Barnett
Attorney General of South Dakota

Paul Summers
Attorney General of Tennessee

John Cornyn
Attorney General of Texas

William H. Sorrell
Attorney General of Vermont

Iver A. Stridiron
Attorney General of U.S. Virgin Islands

Christine O. Gregoire
Attorney General of Washington

Darrell V. McGraw Jr.
Attorney General of West Virginia

James E. Doyle
Attorney General of Wisconsin

Hoke MacMillan
Attorney General of Wyoming