Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the	)	
Telecommunications Act of 1996:	)	
	)	
Petition for Rulemaking to Enhance	)	RM-11277
Security and Authentication Standards	)	
For Access to Customer Proprietary	)	
Network Information	)	

OPPOSITION OF BELLSOUTH CORPORATION

BellSouth Corporation, on behalf of its wholly-owned affiliated companies ("BellSouth"), submits this Opposition to the Petition for Rulemaking filed by the Electronic Privacy Information Center ("EPIC Petition"), assigned to the above referenced Consumer and Governmental Affairs Bureau rulemaking proceeding.[1]

In its Petition, EPIC requests that the Commission initiate a rulemaking proceeding "to establish more stringent security standards for telecommunications carriers in releasing Consumer [sic] Proprietary Network Information ('CPNI')."[2] EPIC asserts that such a rulemaking is necessary because of the supposed illegal actions of "third party data brokers and private investigators that have been accessing CPNI without authorization."[3] Stated differently,

---

1 *See Consumer and Government Affairs Bureau Reference Information Center Petition for Rulemakings Filed, Public Notice*, Report No. 2726 (rel. Sept. 29, 2005).

2 EPIC Petition at 1. The defined term in Section 222(f)(1) of the Communications Act of 1934, as amended, is "customer proprietary network information" or "CPNI."

3 EPIC Petition at 1. EPIC's position that customer information is being improperly accessed and/or disclosed is based primarily on website advertising of these same "third party

EPIC requests that telecommunications carriers be required to spend millions of dollars to address the illegal and improper activities of parties over which the carriers have no control. BellSouth opposes EPIC's request for a rulemaking for several reasons, including the fact that (1) existing law and Commission rules adequately address the issues raised by EPIC; (2) carriers such as BellSouth have already instituted appropriate procedures to protect the confidentiality of customer information; (3) the "solutions" proposed by EPIC[4] are either unreasonably costly or are already voluntarily in use by many telecommunications carriers; and (4) EPIC proposes to impose significant burdens on carriers that may be innocent victims of misrepresentation, fraud and theft, while failing to address those engaged in bad acts.

As EPIC notes, telecommunications carriers are already subject to clear and unambiguous obligations to guard the confidentiality of CPNI and to ensure that it is not disclosed to third parties without customer approval or as required by law.[5] Telecommunications carriers have "a duty to protect the confidentiality of proprietary information of, and relating to . . . [their] customers"[6] and are prohibited from allowing third parties to have access to CPNI "[e]xcept as

---

data brokers and private investigators." The EPIC Petition includes copies of pages taken from these websites and concludes that "it appears that these violations are occurring at an alarming rate" because of the cost of maintaining and establishing a website, the inclusion of online advertising and the establishment of contacts with other investigators. "Combined, these factors and the large number of entities offering call records online suggests [sic] that many individuals' phone records are being illegally access [sic] and sold every day simply to cover the cost of doing business." *Id.* at 7, 8. EPIC asks that significant new burdens and requirements be imposed on telecommunications companies based on a problem assumed to exist because of the advertising of these third parties.

4 *Id.* at 11.

5 *Id.* at 2-3.

6 47 U.S.C. § 222(a).

required by law or with the approval of the customer."[7] Carriers such as BellSouth have instituted practices and procedures designed to meet their obligations under the current law. In fact, these carriers are required to provide a certification to that effect on an annual basis.[8]

BellSouth takes these legal obligations seriously and makes all reasonable efforts to protect the confidentiality of this information. All employees who have access to customer information are required to take training on the CPNI confidentiality and use restrictions on a biennial basis. This training makes it clear that customer records can only be accessed for legitimate business purposes and that inappropriate access can and will result in disciplinary action, up to and including termination of employment. This training also addresses "social engineering" or "pretexting," alerting BellSouth's employee base to the possibility that unscrupulous persons may attempt to improperly obtain customer information by misrepresenting their identity. This same training is required of BellSouth's vendors who have access to customer records in the performance of services for BellSouth.

The law already provides a means to address a failure by a telecommunications carrier to meet its obligations under Section 222. If there are bad actors engaged in or facilitating improper access to and use of CPNI, there are adequate avenues to pursue the halt of such activity.[9]

---

7 *Id.* § 222(c)(1).

8 *See* 47 C.F.R. § 64.2009(e).

9 In fact, EPIC is pursuing one of the existing and available means to combat the complained of activity. Attached to the EPIC Petition is a copy of a complaint against Intelligent e-Commerce, Inc. ("IEI") filed with the Federal Trade Commission alleging that IEI is engaged in unfair or deceptive acts or practices under Section 5(a) of the FTC Act and is violating the Telecommunications Act of 1996, as well as the U.S. Postal Regulations. *See* Attachment A to EPIC Petition at 1.

EPIC argues that in the CPNI proceedings to date, the Commission "has focused on the notice and disclosure requirements necessary to disseminate CPNI data to carrier affiliates and third parties for marketing purposes" and did not "adequately address third party data brokers and private investigators that have been accessing CPNI without authorization."[10] These simplistic statements misrepresent the extent to which both Congress and the Commission have addressed issues related to maintaining the confidentiality of proprietary customer information, including CPNI. As noted above, Congress has clearly imposed confidentiality and access prevention obligations on telecommunications carriers. Additionally, contrary to EPIC's assertions, the Commission has addressed these same issues in its rulemaking process. While much of the Commission's CPNI-related activity has been focused on the appropriate processes for internal use of CPNI, the issue of confidentiality has been clearly and consistently addressed by the Commission.[11]

---

[10] Epic Petition at 1, 3-4.

[11] *See Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; 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, *Second Report and Order and Further Notice of Proposed Rulemaking*, 13 FCC Rcd 8061, 8065, ¶ 3 (1998) ("*Second Report and Order*") ("In contrast to other provisions of the 1996 Act that seek primarily to '[open] all telecommunications markets to competition' and mandate competitive access to facilities and services, the CPNI regulations in section 222 are largely consumer protection provisions that establish restrictions on carrier use and disclosure of personal customer information."). *See also Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; 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, *Order on Reconsideration and Petitions for Forbearance*, 14 FCC Rcd 14409, 14413, ¶ 4 (1999) ("*Reconsideration Order*") ("[S]ection 222 requires *all* carriers, whether or not a market is competitive, to protect CPNI and embodies the principle that customers must be able to control their personal information from unauthorized use, disclosure and access by carriers.").

EPIC suggests a series of Commission-mandated "security measures" including consumer-set passwords, audit trails, encryption, notice to affected individuals and the Commission when there is a security breach, and limiting data retention.[12] The Commission has already addressed the issue of "audit trails."

In the *Second Report and Order*, the Commission required that "telecommunications carriers must maintain an electronic audit mechanism that tracks access to customer accounts, including when a customer's record is opened, by whom, and for what purpose. Carriers must maintain these contact histories for a minimum period of one year."[13] Following the Commission's imposition of the "audit trail" requirement, there was a firestorm of industry opposition. This opposition mainly involved concerns with the complexity of customer database maintenance systems, the IT cost associated with modifying systems to meet the requirement and the cost of maintaining databases evidencing access to customer records. Comments submitted in motions for reconsideration of the "audit trail" and other systems safeguards, indicated that the cost of meeting the audit trail requirement for individual carriers ranged up to $270 million.[14] These were cost estimates provided in the late 1990's – today, these cost figures would undoubtedly be significantly increased. In the *Order on Reconsideration*, the FCC eliminated the "audit trail" requirement, writing "[a]s it is already incumbent upon all carriers to ensure that

---

12 EPIC Petition at 11.

13 *See* 47 C.F.R. § 64.2009(c), adopted in the *Second Report and Order* and amended pursuant to the *Reconsideration Order.*

14 *Reconsideration Order*, 14 FCC Rcd at 14472, ¶ 123.

CPNI is not misused and that our rules regarding the use of CPNI are not violated we conclude, on balance, such a potentially costly and burdensome rule does not justify its benefit."[15]

EPIC points to the possibility that systems can be compromised by hackers who gain access to carriers' customer record databases, suggesting that customer records be stored in encrypted form. Not only would this requirement impose additional significant data storage costs, carriers like BellSouth already have data security measures in place designed to be effective in combating inappropriate internal and external access to customer information. For example, the following general security steps are a normal part of BellSouth's procedures for preventing, detecting and dealing with efforts to improperly access customer information, whether via BellSouth's internal network or via the Internet:

- Internet access from contractors/employees is through Internet proxies for logging, content filtering and virus protection;
- inbound Internet access is protected by firewalls, with access by a standard multi-layer architecture access limited by IP address and port (or service);
- authorized third party connections use private lines and are protected by firewalls and/or router filters;
- corporate email is protected by content (SPAM and attachment blocking) filtering;
- application access requires a current user ID and password, with access rights defined and assigned by specific job responsibilities and accounts are aged and removed from the system if not used;
- remote access requires 2 factor authentication to access the network; and

[15] *Id.* at 14475, ¶ 126.

- direct access to BellSouth's network and systems requires entering a user ID and password at the desktop.

EPIC also suggests a mandatory means for confirming the identity of customers when a customer requests information concerning their telecommunications services. Carriers use a variety of means to confirm the identity of the requesting person.[16] It is inappropriate and unnecessary for the Commission to dictate the means by which carriers confirm the identity of callers to call centers or visitors to restricted portions of their websites. Again, pursuit and action against the guilty actors is the proper course of action, not the imposition of costly regulatory requirements on the innocent.

EPIC suggests that burdens be imposed on those who are acting properly rather than pursuit of those who are acting illegally or unscrupulously. There is no evidence that these events occur other than as a result of illegal or improper activity by these data brokers or private investigators. The Commission should not institute a rulemaking in this area. There already exist adequate means to pursue bad actors. Telecommunications carriers, like BellSouth, have already instituted commercially reasonable processes and procedures to protect the confidentiality of customer information.

---

[16] In fact, BellSouth offers its customers the option of using a customer-provided password for use in telephonic contacts and uses customer-provided passwords in its on-line bill service. Customers concerned with inappropriate access can request these additional measures.

Respectfully submitted,

BELLSOUTH CORPORATION

By /s/ Hubert H. Hogeman III
Hubert H. Hogeman III

Its Attorney

Suite 4300
675 West Peachtree Street, N. E.
Atlanta, Georgia 30375
(404) 335-0797

Date: October 31, 2005

CERTIFICATE OF SERVICE

I do hereby certify that I have this 31st day of October 2005 served the following with a copy of the foregoing **OPPOSITION OF BELLSOUTH CORPORATION** via electronic filing and/or by placing a true and correct copy of the same in the United States Mail, postage prepaid, addressed to the parties listed below.

+Marlene Dortch
Office of the Secretary
Federal Communications Commission
The Portals, 445 12th Street, S. W.
Room TW-A325
Washington, D.C. 20554

+Best Copy and Printing, Inc.
The Portals, 445 12th Street, S. W.
Room CY-B402
Washington, D. C. 20554

Chris Jay Hoofnagle
Senior Counsel
Electronic Privacy Information
Center West Coast Office
944 Market Street, #709
San Francisco, CA 94102

/s/ Juanita H. Lee
Juanita H. Lee

+ **VIA ELECTRONIC FILING**