

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

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
IP-Enabled Services	)	WC Docket No. 04-36

**REPLY COMMENTS OF  
THE UNITED STATES TELECOM ASSOCIATION**

**INTRODUCTION**

Companies commenting on the customer proprietary network information (CPNI) rules proposed in the Further Notice of Proposed Rulemaking<sup>1</sup> overwhelmingly rejected the proposal to adopt additional CPNI rules until the Federal Communications Commission has gained substantial experience with the operation of its recent new rules and can assess the consumer costs and benefits of those rules. Until the rules have been implemented and tested to see whether they are sufficient to ensure the protection of customer privacy, there is no need to impose additional rules—which would make it more difficult for consumers to access account information and raise costs for carriers. As Vonage says, “Each additional obligation imposes a layer of complexity on the consumer experience and adds costs to these highly competitive services, and such

---

<sup>1</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking (rel. April 2, 2007).

procedures and costs should only be imposed where there is a demonstrable public interest benefit.”<sup>2</sup>

Only the Consumer Coalition Council (the “Coalition) recommended that the Commission adopt all of the proposed rules and then some. (The New Jersey Rate Council also supports additional regulation.) The United States Telecom Association<sup>3</sup> again urges the Commission to reject recommendations to enact rules requiring carriers to expand password protection, require audit trails, encrypt all CPNI, limit employee access to CPNI, limit data retention, and adopt a comprehensive opt-in policy. Additional rules would burden consumers by making it more difficult for them to access account information and would be costly for carriers. Because there is no current evidence that further regulation would provide a consumer benefit, the Commission should refrain from imposing more regulation.

## **DISCUSSION**

### **Password Protection**

The Coalition would like the Commission to require carriers to implement a mandatory password protocol for the release of *any* customer information—whether or not it is call-detail CPNI. The Coalition does not show that pretexters have exploited the absence of passwords for non call-detail information. It simply asserts that there is a loophole that pretexters could possibly exploit. The Coalition tries to justify

---

<sup>2</sup> Vonage Comments at 2.

<sup>3</sup> USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks.

imposition of this overbroad rule by claiming, for example, that its plan reduces customer confusion by requiring customers to give passwords every time they call customer service for whatever information. These arguments are contrived and miss the point made by USTelecom and every other party commenting in this proceeding: ***There is no current evidence that requiring passwords before any CPNI could be disclosed on customer-initiated calls would provide a consumer benefit to justify the substantial burdens of passwords on customers and carriers.***

In the absence of such evidence, the Commission should refrain from imposing more regulation. Carriers are aware of nothing to suggest that non-call detail CPNI, such as the type of plan or billing method a customer chooses, is sought by pretexters. Yet there is substantial evidence that requiring passwords for customers to access non-call detail CPNI would unnecessarily frustrate consumers, who tend to call infrequently and rarely ask for call detail information. Recalling and providing a password would make it more difficult for customers to efficiently access their accounts, change services, and obtain billing information. Frustrated customers often spend longer periods with customer service representatives, which increases costs for companies. As a result, requiring customers to provide passwords even when they are seeking information that pretexters do not care about would not serve their interests.

### **Audit Trails**

The Coalition asserts that record access should be audited to prevent improper disclosure of personal information maintained by communications companies. The Coalition ignores completely the fact that audit trails are not closely targeted to protecting CPNI and are economically infeasible. As AT&T points out, audit trails are

of little value in ferreting out pretexters because they only show that an employee accessed a customer's account at the request of a person who claimed to be the customer.<sup>4</sup> Furthermore, as USTelecom has noted, audit trails would require significant systems modifications and costs. The last time the Commission considered requiring audit trails in the late 1990s, the cost of complying with the audit trail requirement was estimated to be \$270 million by legacy AT&T.<sup>5</sup> It is likely that costs have only increased in the meantime.<sup>6</sup>

**Internal Safeguards: Encryption, Employee Access, Data Retention**

The Consumer Coalition wants the Commission to require carriers to adopt other internal physical safeguards, such as encrypting CPNI, limiting employee access to CPNI, and limiting data retention. Such requirements are not warranted or advisable as they would limit carriers' ability to choose the most effective and efficient physical safeguards. Carriers must have flexibility to choose the means of physically protecting CPNI, based on their individual systems, technology, and customer needs.

While some USTelecom members such as AT&T, for example, may use encryption in many instances to protect the transfer of CPNI to third parties and require employees, agents, vendors, and others to follow certain security protocols before gaining access to CPNI databases, a one-size-fits-all approach is not the most effective and efficient means of protecting CPNI. The costs of encryption are substantial. For example, Verizon notes that encrypting all CPNI in all of Verizon's systems likely

---

<sup>4</sup> See AT&T Comments at 8.

<sup>5</sup> See USTelecom Comments at 4.

<sup>6</sup> See Comcast Comments at 7.

would cost tens of millions of dollars and yet could not guarantee security of the data.<sup>7</sup> Significantly, these expenditures would do nothing to deter data brokers, who proceed by deceit and impersonation, rather than hacking.

Moreover, the Commission should not mandate data retention limitations as the Coalition argues. CPNI is a broad term that encompasses different types of information, and, therefore, what to retain and for how long varies with the particular data at issue.<sup>8</sup> FCC-imposed limitations on data retention could hinder the availability of data for law enforcement purposes and expose carriers to liability if they cannot maintain records as required by applicable state and federal statutes of limitations. Therefore, the Commission should not add another layer of regulation to the already effective state and federal regulation in this area.

### **Opt-In**

The Coalition wants the Commission to go beyond requiring carriers to obtain customer opt-in consent prior to providing personal information to joint venture partners and independent contractors to requiring a comprehensive opt-in approach for CPNI provided to carriers' agents and affiliates for marketing purposes. USTelecom strongly opposes a comprehensive opt-in requirement because there is no relationship between pretexting and the information used for marketing and no evidence that use of CPNI by agents and affiliates creates vulnerability. Furthermore, an opt-in requirement

---

<sup>7</sup> See Verizon Comments at 16.

<sup>8</sup> See USTelecom Comments at 6. For example, call detail records are relevant for tax purposes, so carriers must comply with a host of federal rules and regulations (including Internal Revenue Service rules and Sarbanes-Oxley requirements) as well as state rules and regulations to develop appropriate retention parameters for these records.

would disrupt efficient business practices without doing anything to eliminate pretexting, would hurt customers by limiting their access to valuable marketing information, and would infringe on carriers' First Amendment rights.

First, there is no relationship between pretexting and customer information used for marketing, such as the type of service a customer has, which package a customer has, or speed of DSL service. There is no evidence that pretexters seek anything but call detail records. Requiring customers' affirmative consent before information may be shared for marketing purposes would not achieve the goal of stopping pretexting.

Second, there is no evidence that use of CPNI by agents and affiliates creates a vulnerability. There are those USTelecom members such as Embarq who do not transfer CPNI but allow their agents to access their systems where CPNI is stored through secure log-ons.<sup>9</sup> This kind of access does not allow access to the entire customer database at one time but only to a record at a time for a specific customer's account. Contracts with telemarketing agents have strict confidentiality clauses requiring immediate termination of the agent and immediate elimination of database access. In any event, it is unlikely that pretexters would call a carrier's marketing affiliates and agents to fraudulently obtain customers' CPNI.

Third, an opt-in regime would disrupt efficient business practices with no corresponding benefit for consumers. USTelecom's larger members have many affiliates. Under an opt-in regime, each affiliate of a USTelecom member would have to obtain duration-of-call (DOC) or permanent affirmative consent before marketing to

---

<sup>9</sup> See Embarq Comments at 4

customers. Because customers rarely give permanent opt-in consent, carriers would have to get DOC consent, which would require their customer service representatives to spend more time and resources with customers on the telephone.

Fourth, a comprehensive opt-in requirement would result in a poor customer experience as the customer would not be aware of the other services and packages carriers have available to them. As Verizon has pointed out, “in practice, opt-in amounts to a ban on target marketing.”<sup>10</sup> In the absence of targeted marketing, carriers would be likely to choose mass marketing, which would result in customers receiving unwanted ads while at the same time making it difficult for customers to sort through the clutter to find the ads for the services and packages they may desire.

Finally, the most compelling reason not to mandate an opt-in regime is that it would infringe on carriers’ First Amendment rights. Supreme Court precedent dictates that a prior restraint on commercial speech must “directly advance[]” the solution of the problem and be narrowly tailored.<sup>11</sup> Because a customer’s opt-in status has no bearing on whether a pretexter can access his or her CPNI from a carrier’s agent or affiliate, an opt-in solution is neither directly material to the government’s interest in protecting CPNI nor narrowly tailored to that goal. Furthermore, even if this proceeding were broader than the pretexting problem, no evidence suggests that CPNI stored at a carrier’s agent or affiliate would be at a heightened risk of exposure to data brokers. As

---

<sup>10</sup> Letter from Donna Epps, Vice President Federal Regulatory, Verizon to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 12 of attached white paper (filed Jan. 29, 2007).

<sup>11</sup> *Id.* at 20, citing *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 477 U.S. 557 (1980).

the Commission has recognized, carriers still have control over CPNI possessed by its affiliates and agents, and “many customers accept and understand that carriers will share their information with affiliates and agents.”<sup>12</sup> Because there is much on the record as to why a comprehensive opt-in requirement would be unconstitutional, the Commission should not adopt an opt-in requirement for affiliates and agents.

### **CONCLUSION**

The requirements recommended by the Coalition would impose substantial burdens on consumers and carriers without offering commensurate benefits. Until the Commission allows the market a chance to balance customer needs for privacy and security with ease of access and efficiency, it should not burden carriers and consumers with additional regulations.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By:  \_\_\_\_\_

Jonathan Banks  
Indra Sehdev Chalk

Its Attorneys

607 14<sup>th</sup> Street, NW, Suite 400  
Washington, DC 20005  
(202) 326-7300

August 7, 2007

<sup>12</sup> Report and Order and Further Notice of Proposed Rulemaking ¶ 40.