BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION

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

COMMENTS OF THE

INDEPENDENT TELEPHONE AND TELECOMMUNICATIONS ALLIANCE

To the Commission:

I. INTRODUCTION

The Independent Telephone and Telecommunications Alliance (ITTA) hereby submits these comments in the above-captioned dockets. In summary, existing Commission rules regarding Customer Proprietary Network Information (CPNI), coupled with the self-interest in proper implementation on the part of carriers subject to them, are sufficient to protect adequately consumer information. The implementation of additional regulations will not augur additional protection of an amount adequate to justify their cost.

The member companies of ITTA undertake rigorous measures to ensure their compliance with Commission rules. The Commission's latest *Further Notice of Proposed Rulemaking*[1] seeks comment on additional CPNI safeguards, but without apparent evidence that would tend to justify imposition of such comprehensive new measures.

The Commission has taken steps to curb improper disclosure of private call-detail information of private consumers and businesses.[2] ITTA participated in the most recent CPNI proceeding, urging regulatory parity among providers of services and cautioning the Commission against the adoption of regulations that would create steep regulatory burdens.[3] Now, the Commission asks whether it should expand new CPNI rules.

II. NOTICED ISSUES

Non-Call Detail Data

The Commission seeks comment on whether CPNI regulations should be extended to non-call detail data.[4] ITTA submits that adequate justification does not exist for extending CPNI requirements to non-call detail CPNI or certain account changes, such as changes in address of record, account plans, or billing methods. The Commission found that enhanced rules for call detail related matters were justified because numerous incidents implicating the sale of call

---

[1] Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (FNPRM).

[2] *See, generally, Id.*

[3] *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Consumer Information: Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information: Ex Parte Presentation of the Independent Telephone and Telecommunications Alliance,* CC Docket No. 96-115, RM 11277 (Dec. 14, 2006).

[4] FNPRM at para. 68.

records had been reported.[5] By contrast, non-call detail information is not the type of information pretexters would pursue, as they are generally interested in call details. Therefore, there is no clear nexus between pretexting and non-call detail information to justify the increased burden and cost of regulations over this type of information.

Imposition of requirements to extend new CPNI regulations to non-call detail information would place an undue burden on carriers, including ITTA mid-size carriers, and customers. In the absence of a reasonable expectation that certain account change information would require password-access, requirements to obtain passwords (or other security mechanisms) would create a nuisance for consumers and additional administrative costs and burden for carriers.

Audit Trail

Likewise, and for similar reasons, the Commission should not adopt audit trail requirements. The Commission asks whether an audit trail would assist law enforcement with criminal investigations against pretexters.[6] The record-keeping associated with every consumer inquiry would be of negligible benefit in the more narrow occurrences of fraud. Presumably, sufficient information from other sources and records to which requirements already apply would provide adequate resources of information for law enforcement. Moreover, the keeping of vast and intricately detailed records of communications and other customer interactions in which largely no misfeasance occurs would simply frustrate necessary efforts when focusing on the occurrences in which actual harm has occurred. A requirement to create and maintain unneeded information would risk diverting resources from those matters that require more careful

[5] FNPRM at para. 12-14.

[6] FNPRM at para. 69.

attention. It is not apparently likely that consumers are often enough the victims of schemes in which the billing address of their account or their service plans are changed surreptitiously, resulting in harm.

Audit trails are expensive and will not prevent pretexting. It would simply create a requirement to maintain vast amounts of information that for the most part is of no real value or use to a company. In fact, the Commission recognized, "Our current record indicates that the broad use if audit trails likely would be of limited value in ending pretexting because such a log would record enormous amounts of data, the vast majority of it being legitimate customer inquiry."[7] ITTA agrees, and urges the Commission to refrain from imposing audit trail requirements.

Safeguards for Physical Data

With regard to the inquiry regarding safeguards geared toward the physical treatment of CPNI,[8] ITTA submits that physical safeguard requirements are not warranted. In the first instance, specific rules related to types of data and mode of transport and/or transfer would require finely-detailed approaches, justified by the relative risks presented by each mode of transport. By contrast, carriers currently have adequate incentive to ensure that the transport, transfer, and exchange of CPNI is treated with due care; unauthorized disclosure of CPNI subjects the carrier to penalties arising out of violation of the Commission's rules. Carriers are aware that, as the Commission has noted, the "Act imposes on them the duty of instituting

[7] FNPRM at para. 69.

[8] FNPRM at para. 70.

effective measures to protect of the privacy of CPNI."[9] In fact, the Commission's new CPNI rules now shift the burden of proof to the carrier to prove that it has adequate protections in place. The Commission stated, "[W]e hereby put carriers on notice that the Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer's CPNI that the carrier did not sufficiently protect that customer's CPNI."[10] This stricter liability provision itself should serve to further increase the level of care given to CPNI. The incentive, therefore, to protect the information is present; adequate and appropriate safeguards exist, and the threat of penalties for unlawful disclosure is adequate to create carrier-enacted safeguards, rather than government-mandated guidelines.

III. CONCLUSION

In light of existing regulations that are themselves comprehensive, and carriers' self-interest in adhering to those rules to protect their customers and maintain compliance with applicable regulations, ITTA submits that additional CPNI requirements as described above are not necessary and should not be imposed.

Respectfully submitted,

s/*Joshua Seidemann*
Joshua Seidemann
Director, Regulatory Policy
Independent Telephone and Telecommunications Alliance
975 F Street, NW, Suite 550
Washington, DC 20004
202/552-5846
www.itta.us

DATED: July 9, 2007

[9] FNPRM at para. 35, citing 47 USC 222(c) and 47 CFR 64.2009.

[10] FNPRM at para. 63.