

**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

**COMMENTS
OF
THE IOWA TELECOMMUNICATIONS ASSOCIATION**

I. INTRODUCTION

The Iowa Telecommunications Association (ITA)¹ hereby submits these comments in response to the Commission's Further Notice of Proposed Rulemaking (Further NPRM)² in the above-captioned proceeding. The Further NPRM seeks comment on whether the Commission should act to expand its CPNI rules further, and whether it should expand the consumer protections under those rules to ensure that customer information and CPNI are protected in the context of mobile communications devices. ITA respectfully submits that further expansion of the Commission's CPNI rules

¹ ITA is the nation's largest and second oldest state telecommunications association. It includes within its membership 141 Iowa incumbent local exchange carriers (ILECs), which constitute all of the ILECs serving Iowa except Qwest Corporation, Iowa Telecommunications Services, Inc. and two independent carriers. ITA's membership also includes several competitive local exchange carriers (CLECs) and Iowa's statewide centralized equal access provider, Iowa Network Services, Inc. The median number of access lines served by Iowa ILECs is slightly more than 1,100, and more than 100 of ITA's member companies serve fewer than 2,000 access lines.

² *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information* CC Docket No. 96-115; *IP-Enabled Services* WC Docket No. 04-36, 22 FCC Rcd 6927 (released April 2, 2007).

is unwarranted and will impose unreasonable costs of compliance and overly burdensome obligations on small carriers and the rural customers they serve. The Commission's recently strengthened CPNI rules are more than sufficient to ensure that small carriers meet or exceed their customers' reasonable expectations regarding privacy safeguards and the security of CPNI. Rather than being compelled to implement additional safeguards, small carriers should be permitted maximum flexibility to work within the Commission's recently strengthened CPNI rules to protect the privacy of customer CPNI and to cooperate with the Commission and law enforcement agencies in identifying, reporting and prosecuting pretexters and other bad actors.

II. COMMENTS

The member companies of ITA are primarily small ILECs with a history of providing high quality telecommunications services to rural customers. In most cases, the owners and employees of these companies live and work in the same communities as their customers and coworkers. To the extent small carriers have been or may be targeted by pretexters or other bad actors, this unique familiarity serves as a first line of defense in protecting customer privacy.

The privacy of customer information and CPNI is being further advanced by carrier implementation of the additional safeguards recently adopted by the Commission. As the Commission has appropriately suggested, any additional regulations must be balanced against the additional burdens that would be placed on small carriers and their customers. ITA is unaware of any evidence that pretexters have targeted small carriers or that existing safeguards will be insufficient to protect CPNI in a reasonable and effective manner. For small carriers, the well-publicized customer privacy lapses of large national carriers create clear business and legal incentives to meet or exceed the Commission's recently reinforced standards. Accordingly, ITA opposes the adoption of any additional safeguards that would divert limited financial and human resources with little or no additional benefit to consumers.

A. Mandatory Password Protection for Non-Call Detail CPNI would be an Undue Additional Burden for Small Carriers and Unpopular with Customers.

The Commission's CPNI rules recognize a distinction between call detail and non-call detail CPNI.³ This distinction is directly related to the documented disclosure of call detail CPNI to so-called pretexters and other bad actors in a manner that presents an immediate risk to customer privacy.⁴ Subject to alternative methods of customer verification, the existing rules mandate password protection for the release of call detail information in response to customer-initiated telephone contact.⁵ While the Commission asserts that required password protection and verification procedures will amount to a minimal inconvenience for carriers and consumers, the existing customer authentication requirements extend to call detail and non-call detail CPNI and are expected to have a significant impact on many commonplace interactions between small carriers and their customers. In many instances, password protection requirements may in fact serve as a hindrance to efficient customer service and an infringement on customers' legal rights to have readily available access to their CPNI.

To the extent password protection may be justified in the context of call detail information, the justification and corresponding benefit of such safeguards with respect to such information will be less apparent to those customers who will be inconvenienced by such a requirement. In the interests of customer service, small carriers should retain the flexibility to determine (based on their customer service capabilities and the individual preferences of their customers) whether or not to provide password protection for customer-initiated inquiries regarding non-call detail information. The Commission's current CPNI rules require carriers to take all necessary measures to immediately notify customers of certain account changes, regardless of whether those changes involve call detail or non-call detail CPNI.⁶ For small companies operating in rural communities,

³ Further NPRM at ¶13.

⁴ *Id.*

⁵ *Id.* at ¶¶15-17.

⁶ 47 C.F.R. §64.2010(f).

rules requiring additional password protection for non-call detail information would serve little purpose and would be inconsistent with customers' expectations for fair and reasonable customer service. Given the limited value of non-call detail information to pretexters and other bad actors, optional password protection is sufficient to balance the customer service interests of carriers and consumers with the public interest in maintaining the security of non-call detail CPNI.

B. The Burdens of Requiring Audit Trails to Track the Disclosure of CPNI and Carrier/Customer Contact would far Outweigh the Limited Benefits to Customers and Law Enforcement.

As with other customer service functions, the recordkeeping practices of small carriers may vary considerably from company to company. Few, if any, of the small carriers represented by ITA have systems capable of creating extensive audit trails for tracking all customer contact as suggested in the Further NPRM. Additionally, many small carriers operate in small, rural communities where contact between customers and company employees often occurs outside of business hours and is not limited to interactions between customers and dedicated customer service personnel. In Iowa, a typical ILEC has fewer than ten (10) total employees on staff, with an average of two (2) or (3) of those employees dedicated to customer service and recordkeeping functions. In light of these and other factors, extensive audit trails are not generally used by small carriers to track customer contact.

Any requirement imposing extensive audit trail capability would force small carriers to invest their limited financial and human resources in necessary technical upgrades and customer service training with little or no benefit to consumers. For carriers required to upgrade their current software systems, the costs of compliance would be prohibitive and, to the extent not passed directly on to customers, may delay network improvements. While many billing providers have the capability to track certain account access and service order activity, extensive software upgrades would be required

in order to properly detect and log all access to CPNI.⁷ As accurately suggested in the Further NPRM, the volume of data resulting from such audit trails would be immense and would be of limited value in protecting the privacy and security of customer CPNI. In the rare instances where law enforcement agencies may otherwise benefit from extensive audit trails relating to atypical account activity, the current customer service and recordkeeping practices of many carriers are likely to provide the same types of information on a more manageable scale. In any case, the limited benefits of audit trails would not justify the enormous cost and service burdens imposed on small carriers.

C. Rules Establishing Mandatory Physical Safeguards for the Transfer of CPNI among Companies would be Overly Invasive and of Minimal Benefit in Protecting CPNI.

The business practices of small carriers with respect to the transfer of CPNI between a carrier and its affiliates or other third parties authorized to access or maintain CPNI vary from company to company, often depending on the business relationship, the identity and technical capabilities of the parties to the business relationship, and the source and sensitivity of the CPNI being shared. Small carriers are not unmindful of their responsibility to protect customer CPNI from unauthorized disclosure, including in the context of information sharing arrangements between a carrier and its affiliates or authorized third parties. A majority of these relationships involve appropriate contractual language and cost-effective best practices for the transfer of or allowance of access to CPNI. In light of the recently heightened responsibility of carriers under the Commission's revised CPNI rules, many small carriers are reviewing their existing business practices to ensure ongoing compliance.

To the extent such a requirement would dictate carrier business practices that may or may not be cost effective in a given situation, any rule imposing specific physical

⁷ In response to an inquiry from ITA's Industry Relations Committee, Mid America Computer Corp. (MACC) has estimated that the cost of audit trail requirements would approach \$2,000 - \$3,000 per access line for small ILECs. MACC provides billing, data processing, statement printing and fulfillment, carrier access billing solutions (CABS) and training services to many ITA member companies. For more information about MACC, refer to www.maccnet.com.

safeguards on the transfer of or access to CPNI would be overly invasive. Depending on the scope of the requirement, the implementation of mandatory encryption, audit trails, data logs, etc. may result in significant financial costs to small carriers. In many cases, small carriers will be unable to justify these compliance costs, effectively eliminating their ability to transfer or share access to CPNI as otherwise permitted or required by law, including for efficient and beneficial service to customers. The benefits of mandating specific physical safeguards are speculative at best. In the absence of any direct evidence that physical safeguards currently employed by small carriers are insufficient to protect CPNI, the Commission should refrain from expanding its CPNI rules in any manner that would impose additional costs of compliance on small carriers.

D. Rules Limiting Carrier Data Retention would be Overly Invasive and of Minimal Benefit in Protecting CPNI.

As with mandatory physical safeguards, a "cookie cutter" approach to carrier data retention will force small carriers to alter their current business practices with little or no benefit to consumers. In many instances, CPNI is or may be commingled with customer data that a carrier is required to retain under the Commission's data retention rules or corresponding state data retention requirements. Many small carriers will face significant costs if they are required to develop and maintain systems capable of separately isolating and destroying or de-identifying customer records containing CPNI. In most instances, this aged CPNI will be of little or no value, and the destruction of such records will do little or nothing to enhance the protection of the categories and types of CPNI targeted by pretexters. ITA shares the concern of law enforcement agencies regarding the impact that carrier destruction of customer records may have on the ability of such agencies to conduct and prosecute criminal and other lawful investigations, including investigations against pretexters. Again, in the absence of any direct evidence that changes in data retention policies are necessary to the protection of CPNI, the Commission should refrain from expanding its CPNI rules in any manner that would impose additional costs of compliance on small carriers with little or no benefit to consumers or the public interest.

E. The Commission should Refrain from Imposing Mandatory Burdens on Wireless Carriers for the Protection of CPNI Stored within a Customer's Mobile Communications Device.

In response to customer demand for advanced communications services, small carriers increasingly offer wireless communications services in rural areas. In the context of this customer/carrier relationship, mobile communications equipment is almost exclusively the property of the customer, and wireless carriers should not be saddled with legal responsibility for the removal of CPNI from such equipment. For small carriers lacking economies of scale, any financial burden or potential legal liability associated with wireless devices would serve as a deterrent to carriers' willingness or ability to accept or service wireless devices from certain manufacturers or under certain circumstances. Such a result would be detrimental to customers living in rural areas with limited access to other means of technical assistance. To the extent that any such requirements are shown to be reasonable and cost effective, uniform standards for the configuration of wireless devices so that consumers can easily and permanently delete personal information may be helpful in assisting customers with their personal responsibility to delete CPNI prior to discarding their devices. In that case, wireless carriers should be free to assist customers with such functions without undue exposure to legal or financial liability related to customer CPNI stored within the customer's wireless devices.

III. CONCLUSION

The Commission's existing CPNI rules are sufficient to ensure that small carriers are able to appreciate and fulfill their legal responsibilities to safeguard CPNI and to protect customer privacy in a reasonable and effective manner. Rather than focusing time and resources on compliance with additional carrier regulations, these carriers should now be permitted to focus on cooperative efforts with the Commission and law enforcement agencies that will result in the continued identification and punishment of pretexters and other bad actors. None of the additional safeguards contemplated in the Further NPRM are necessary to these efforts. Before imposing any additional

regulations on small carriers, the Commission should be certain that compliance will not be overly burdensome and that the benefit to consumers will exceed the costs of compliance. The burdens of requiring mandatory password protection for non-call detail CPNI and requiring audit trails to track the disclosure of CPNI would impose excessive burdens and would be of limited benefit to carriers, customers and law enforcement agencies. Likewise, rules establishing mandatory physical safeguards for the transfer of CPNI among companies and limiting carrier data retention would be overly invasive and may in fact be detrimental to the interests of carriers, customers and law enforcement agencies. Finally, mandatory burdens on wireless carriers for the protection of CPNI stored within a customer's mobile communications device would unduly shift the responsibility for such safeguards from the customer to the carrier, resulting in the potential for undue financial or legal liability on the part of carriers.

Respectfully submitted,

IOWA TELECOMMUNICATIONS ASSOCIATION

DAVIS, BROWN, KOEHN,
SHORS & ROBERTS, P.C.

By: /s/ John C. Pietila

John C. Pietila

JohnPietila@davisbrownlaw.com

Its Attorneys

The Financial Center
666 Walnut Street, Suite 2500
Des Moines, IA 50309-3993
(515) 288-2500 - telephone
(515) 243-0654 - facsimile
JohnPietila@davisbrownlaw.com

CERTIFICATE OF SERVICE

I, John C. Pietila, hereby certify that copies of the foregoing Comments of the Iowa Telecommunications Association in CC Docket No. 96-115 and WC Docket No.04-36 were sent on July 9, 2007, via electronic mail, to the persons listed below.

/s/ John C. Pietila

John C. Pietila

Janice Myles
Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
Janice.myles@fcc.gov

Best Copy and Printing, Inc.
fcc@bcpiweb.com