

**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
	)	

To: The Commission

**COMMENTS OF RURAL CELLULAR ASSOCIATION**

Rural Cellular Association (“RCA”)<sup>1</sup>, by its attorneys, respectfully submits its comments in response to the Commission’s *Further Notice of Proposed Rulemaking* in the above-captioned proceeding seeking input on means to further protect the privacy of customer proprietary network information (“CPNI”) that is collected and held by communications carriers. *See Report and Order and Further Notice of Proposed Rulemaking*, CC Docket No. 96-115, WC Docket No. 04-36, released April 2, 2007 (“*Report and Order*” or “*FNPRM*”). The proceeding is intended to determine whether the Commission should impose further protections of customer information and CPNI in addition to those safeguards adopted in the *Report and Order*, and whether to adopt supplemental measures to ensure protection against unauthorized access and disclosure of information in the context of mobile communication devices.

---

<sup>1</sup> RCA is an association representing the interests of nearly 100 small and rural wireless licensees providing commercial services to subscribers throughout the nation. Its member companies provide service in more than 135 rural and small metropolitan markets where approximately 14.6 million people reside. RCA was formed in 1993 to address the distinctive issues facing wireless service providers.

RCA opposes imposition of additional regulatory burdens, particularly as applied to small and regional wireless carriers.<sup>2</sup>

## **I. Additional CPNI Protective Measures**

RCA offers comment on the additional measures to protect CPNI discussed in the FNPRM:

### ***A. Password Protection.***

Security of CPNI will be increased by the FCC's newly adopted mandate to use passwords to access an online account, and when customers call the carrier to access call-detail CPNI. However, a further mandate for use of passwords in the provision of non-call detail CPNI and account changes would be burdensome. Small and regional carriers can protect CPNI in ways better than expending resources to force subscribers to remember passwords for communications with the carrier.

The carrier should be permitted to choose whether or not to adopt a password system applicable to non-call detail CPNI and account changes such as address of record, account plans and billing methods. Considerations are that some customers will be discouraged from dealing with the carrier due to the password obstacle. The password may result in persons contacting the carrier to ask about switching to a more advantageous calling plan and being told this cannot be discussed without a password. There will be confusion over which discussions require a password and which do not. Requiring customers to remember yet another password in facilitating a critical service may be especially burdensome on the elderly population.

Offering additional password protection, even if only to those customers who want them,

---

<sup>2</sup> RCA's wireless carriers operate in rural markets and in a few small metropolitan areas. No member has as many as 1 million customers, and the vast majority of RCA's members serve fewer than 500,000 customers.

places another administrative burden on many small and regional carriers. Billing screens must be reconfigured and software upgraded and maintained to make and keep systems compatible with all details of a password requirement. Administrative personnel must be added to design the new process and train all customer service representatives (“CSRs”). Subscribers must be contacted and worked with individually to set password protection by inputting passwords and personal information. This is necessary because many customers will not or cannot set up passworded accounts and records on their own without assistance. If they seek assistance from personal acquaintances, the security of the password system is compromised.

Many RCA members are already in the process of implementing voluntary password systems, giving customers the option to self-manage their security levels and to view and modify their account information. These systems are very expensive, and are best set up as new systems rather than retrofitted onto working platforms. They are best adopted when the carrier has the funds and manpower to accomplish the upgrade, not before the carrier is fully prepared to handle the costs and devote the required attention to the project.

Due to the administrative burdens and other disadvantages of passwords, the choice of whether to implement additional password systems should be left to the carrier and its customers.<sup>3</sup>

***B. Audit Trails.*** Audit trails are not generally used by small carriers to track customer contact. Keeping records of disclosure of CPNI and of all customer contact would be fruitless and expensive. Recordkeeping does not protect CPNI. Audit trails do not prevent unlawful disclosure. The benefit to law enforcement is speculative, and the cost to carriers would be

---

<sup>3</sup> If the Commission nevertheless decides to expand password requirements RCA requests that the Commission also allow any carriers that are willing to establish a customer waiver procedure to provide non-call detail forms of CPNI to a customer’s designated representative who provides the correct password. This would allow, for example, an infirm elderly customer to designate a family member to interact with the carrier on most account matters.

enormous. Carriers would have to maintain mounds of logs of legitimate customer inquiries. Management of that much information would slow down processing of customer requests, require additional personnel and drive up subscriber's costs for service.

Audit trail requirements would be costly and time consuming, and make CPNI no more secure. A log system for all accounts would be burdensome and time-consuming for both the carrier and the customer. Capital costs would be high for software systems to handle ongoing logs as audit trails. Maintaining a log of all CPNI disclosure and customer contact, including legitimate customer inquiries, would require material changes in customer management systems, necessitating additional capital expenditures. Capital costs would be exceeded by administrative costs to log and maintain each instance of a customer contact with a CSR. The cost could be significant depending upon the length of the call or visit and nature of the inquiry. Each contact would have to be logged onto a computerized tracking system, the information catalogued and made available for retrieval. None of this expense and activity increases the protection of CPNI. The more the information is handled, the more likely it is to be mishandled.

RCA opposes audit trails as an unnecessary cost for negligible benefit.

**C. Physical Safeguards.** The FCC should refrain from adopting rules governing the physical transfer of CPNI among companies authorized to access or maintain the CPNI. Physical safeguards should be left to the companies, including their chosen methods of encryption, audit trails, logs, etc. It is in their interest to protect the material. Mandated forms of security would simply invite pretexters to anticipate and defeat the security system. Carriers are in the best position to assess the risk and conform protective barriers to the context and location of the CPNI data.

Mandating methods of safeguarding the transfer of CPNI could negate some of the measures already used by carriers, detract from the creativity of local managers and divert funds to mechanisms that may or may not improve a particular carrier's protective techniques. Additional mandated safeguards would add to carriers' capital costs and affect software systems. They would involve expensive auditing and administrative costs to detail and maintain new processes and not necessarily improve the safety of CPNI being transferred to or accessed by authorized parties. It is safer and more efficient for the authorized parties to agree to and abide by additional safeguards to protect CPNI security. They are the parties with the most knowledge about the risks involved in what they do with the data. The Commission should refrain from imposing additional mandates for physical security of CPNI. Decisions regarding supplemental safety of transferred and accessed CPNI belonging to the carrier should be left to the carrier.

***D. Limiting Data Retention.*** The length of time carriers retain customer records should remain at their discretion, not limited by federal mandate. To mandate in advance which records should be kept for how long, and what exactly are the exceptions, is not within the competence of the FCC or participants in this proceeding. Premature destruction of records could hamper law enforcement efforts by destroying evidence useful to criminal investigations, and intrude on the carrier-customer relationship by destroying data needed to resolve customer billing disputes.

On the other hand, requiring carriers to keep customer data for an extended amount of time because law enforcement might need access to it, and for no other business reason, increases carriers' risk that some data could be improperly released, subjecting carriers to CPNI rule violations. Carriers' own data retention criteria adequately balance the need for customer billing resolution and criminal investigations and cannot be improved by new federal regulations.

Stored data is not easily subject to pilfering of CPNI. Access is extremely limited. Small and regional carriers have existing controls over access to stored data by personnel. Customers have no access to stored data. Customers do, however, expect their carriers to keep records for long periods of time. Customers have been known to use the carrier's lack of documentation as a reason not to pay their bills. Carriers should determine their own practices for routine destruction of data, according to their circumstances and any directly expressed interest of law enforcement.

Enforced limitation of call retention data is not likely to make CPNI more secure. It will only add to the regulatory costs and burdens of small carriers.

## **II. Protection of Information Stored in Mobile Communications Devices**

The privacy of customer information stored in mobile communications devices is a matter of interest to small wireless operators. Most small carriers currently do not refurbish mobile equipment. Small carriers do typically erase customer information from wireless handsets before they are sent out for repair, or are re-used for any reason, such as for loaners to subscribers whose phones are being repaired. Naturally, if the phone cannot be turned on, the data cannot be expunged.

Small carriers do not routinely instruct customers how to permanently erase their personal information before discarding the device. The vast number of handset models makes it impossible for a rural carrier to decipher and explain all actions necessary to purge all personal data from every device. Because most customers are technically challenged and are prone to misplacing the information, small carriers have not made a practice of trying to teach expunging techniques to the general customer base.

Carriers should not be required to erase a customer's personal information or to provide instruction to customers. Customers should follow instructions from the manufacturer of the

device. The customer thereby avoids the circumstance of other parties having access to the information before erasing it, and carriers avoid the risk of false accusations of misuse. The easier manufacturers can make it for customers to permanently erase information the better (although RCA does not favor FCC mandates in this regard). Users would benefit from not having to be dependent upon the honesty and expertise of another to erase the data.

Small carriers would be disadvantaged by a requirement to fully expunge existing customer data from a mobile device at the customer's request. The costs of doing so may exceed the value of the device. If the task is so complicated that it cannot be performed by the average customer, it is likely that the labor, time and liability of the carrier will far outweigh the cost of destroying the device or replacing it with a new one. Rather than require carrier compliance with the customer's request to fully and permanently expunge all personal information, the FCC should permit small carriers the more economical option of destroying or replacing the device, depending upon the customer's circumstances and reason for the request.

### **III. Conclusion**

RCA opposes the imposition of new regulatory burdens on small and regional carriers. The carrier/customer relationship involving the use of passwords is best managed on the local level. New mandates for audit trails, physical safeguards and data destruction would add to the cost of provision of services in rural areas and reduce the competitiveness of smaller carriers. RCA members presently provide CPNI with extraordinary protection, and FCC rules adequately define the regulatory responsibilities of the communications industry. The additional measures set forth in the FNPRM are helpful suggestions; at the same time they are not necessary to the protection of CPNI. The Commission is reasonable in asking for comment rather than adopting additional rules, and should continue to exercise restraint in exercise of its authority.

Carriers serving rural areas need to absorb the FCC's newest requirements rather than be layered with further requirements carrying high costs and unproven benefits. The FNPRM has brought attention to additional forms of CPNI protection. The additional measures will be adopted by carriers as the benefits are recognized and the benefit justifies the cost.

Respectfully submitted,

**RURAL CELLULAR ASSOCIATION**

*[filed electronically]*

David L. Nace  
Pamela L. Gist  
*Its Attorneys*

LUKAS, NACE, GUTIERREZ & SACHS, CHARTERED  
1650 Tysons Boulevard, Suite 1500  
McLean, Virginia 22102  
(703) 584-8678

July 9, 2007