

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)	
)	
Implementation of the Telecommunications)	
Act of 1996:)	CC Docket No. 96-115
)	WC Docket No. 04-36
)	
Telecommunications Carriers' Use of)	
Proprietary Network Information and Other)	
Customer Information)	
)	
IP-Enabled Services)	(FNPRM FCC 07-22)

COMMENTS OF THE NEW JERSEY
DIVISION OF RATE COUNSEL

Ronald K. Chen, Esq.
Public Advocate of New Jersey

Kimberly K. Holmes, Esq.
Acting Rate Counsel
Christopher White, Esq.
Deputy Public Advocate
31 Clinton Street, 11th Floor
Newark, New Jersey 07171
973-648-2690

Dated: July 9, 2007

I. Introduction

The New Jersey Division of Rate Counsel submits comments in response to the Further Notice of Proposed Rulemaking (“FNPRM”) issued by the Federal Communications Commission (“FCC”) in the above-captioned proceeding issued on April 2, 2007.¹ The FNPRM seeks comment on the need for and the appropriateness of further regulations governing the protection of Customer Proprietary Network Information (“CPNI”). Rate Counsel supports the already increased protections the FCC adopted in its order. This FNPRM identifies areas wherein more protections may further the public interest and the protection of consumers’ privacy interests. Review and consideration of such issues are timely and appropriate in an environment where consumers expand their use of communications technologies, and entrust personal and sensitive information to providers of telecommunications and information services.

II. BACKGROUND

QUESTIONS RAISED BY THE FURTHER NOTICE OF PROPOSED RULEMAKING

The Federal Communications Commission (“FCC”) asks for comment on whether the FCC should expand its CPNI rules in various areas, and whether to apply these rules to the area of mobile communication devices.² In terms of expanded password protection, the FCC asks for comment concerning:

- Requiring password protection for non-call detail CPNI;

¹ / *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36, Rel. April 2, 2007 [hereinafter “CPNI Order”].

² / *Id.* at ¶ 67.

- Requiring password protection for all non-call detail CPNI, or only certain types of account changes;
- If only certain account changes require password protection, what are those changes; and
- The effect the new rule will have on carriers.³

The FCC also asks for comment on the need and appropriateness of audit trails. The current rules do not address this issue but the FCC submits that important public issues are implicated in this issues. With respect to audit trails, the FCC asks:

- Should the FCC require audit trails;
- Do carriers currently maintain audit trails tracking customer contact;
- The costs and benefits of tracking disclosures of CPNI and customer contact;
- The utility of audit trails in criminal investigations; and
- Has the technology changed that would ease the costs or burdens of audit trails.⁴

The FCC also requests comments in considering whether to adopt rules that regulate the physical transfer of CPNI by a carrier to a third party with authorized access, including parties maintaining or managing CPNI, joint venture partners, and independent contractors. Specifically, the FCC asks:

- What physical safeguards are currently in place to protect CPNI transfer or disclosures;
- Are the current physical safeguards sufficient;
- What physical safeguards should be required to protect CPNI in these data transfers or disclosures; and
- What will be the costs and benefits of requiring various physical safeguards?⁵

Finally, the FCC seeks comment on whether it should impose data retention requirements on carriers. Specifically:

- The length of time a carrier may retain customer records;

³ / *Id.* at ¶ 68.

⁴ / *Id.* at ¶ 69.

⁵ / *Id.* at ¶ 70.

- Requiring all records be destroyed or only the records of a category of customers which is more susceptible to abuse; and
- Creating exceptions where a carrier can retain records.⁶

In addition, the FCC asks for comment on whether there is a need to expand CPNI protections into the area of Mobile Communications Devices. The FCC wants comment on:

- What CPNI protections currently exist for mobile devices;
- Do carriers currently erase customer information from refurbished equipment, and if so, what methods are used;
- Requiring carriers to permanently erase or allow customers to personally erase customer information;
- Requiring manufacturers to configure their products to allow customers to permanently delete personal information; and
- The cost to carriers of all size in requiring carriers and manufacturers “to fully expunge existing customer data from a mobile device at the customer’s request.”⁷

III. THE PUBLIC INTEREST REQUIRES THAT THESE ISSUES BE FULLY ADDRESSED AND CONSIDERED ON A FULL AND COMPLETE RECORD

Rate Counsel previously submitted comments in this proceeding, and repeats what the overriding public interest considerations should be:

- require telecommunications carriers to notify customers when a request for their CPNI is made before releasing the CPNI
- maintain adequate records of such requests
- adopt more pro-active safeguards—that do not place the onus on consumers—for the prevention of unauthorized disclosure of CPNI
- establish reasonable retention period(s) (but require retention of billing records in back up files to address billing disputes for longer periods)⁸

⁶ / *Id.* at ¶ 71.

⁷ / *Id.* at ¶ 72.

⁸ / *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Consumer Information*, CC Docket No. 96-115; *Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, RM-11277, Comments of the Division of the Ratepayer Advocate (April 28, 2006). Rate Counsel was formally called the Ratepayer Advocate.

Rate Counsel supports the FCC's effort to improve CPNI protection, and believes that the recent rulemaking has in fact advanced the public interest by imposing reasonable and measured requirements while not imposing the burdens of such rules on consumers. The FCC, however, should go farther to protect consumers by exploring the need for, the costs to the public and industry of requiring audit trails and obtain input from all stakeholders on the appropriate data collection and retention periods. Rate Counsel also recommends that the rationale of the existing rules logically extend to the expansion of CPNI protections to non-call detail, and requiring mobile device manufacturers to provide consumers a means of insuring that their personal information can be efficiently deleted from mobile equipment or be protected by use of passwords in the software of such mobile devices.

IV. THE FCC SHOULD FOLLOW COMMISSIONERS COPPS AND ADELSTEIN'S RECOMMENDATIONS TO GIVE GREATER CLARITY TO THE REGULATIONS CONCERNING NOTICE TO CUSTOMERS ONCE CUSTOMER CPNI HAS BEEN BREACHED.

Both Commissioner Copps and Commissioner Adelstein have correctly stressed in strong public policy of ensuring timely and reasonable notice to customers of unauthorized CPNI access. Rate Counsel agrees that in order to adequately protect customers, the rules regarding notice must be clarified and strengthened.

While it is important to allow law enforcement the ability to effectively investigate criminal activity, especially in the area of cyber fraud and identity theft. Commissioner Copps' concern is that notice delays now sanctioned (up to 14 days) may actually be counter productive, may impede effective assistance to law enforcement, and

may in practice harm consumers.⁹ Similarly, the current rules may afford law enforcement too much discretion in delaying notification to customers. Commissioner Adelstein echoes these concerns, and adds that the discretion granted to law enforcement may compromise the FCC's statutory authority.¹⁰

Rate Counsel agrees with Commissioner Copps and Commissioner Adelstein that the FCC should do more in this area and use this proceeding to develop appropriate standards for determining when law enforcement should and can delay the notification to affected customers. The FCC should attempt to define and identify what exigencies justify not immediately informing a customer when CPNI information has been compromised.

V. THE NEW RULES SHOULD EXTEND TO COVER NON-CALL DETAIL CPNI

Password protection should be required to access non-call detail. Restricting password requirements to call records may be insufficient and fall short of adequately protecting a person's privacy. Rate Counsel urges the FCC to reject views that call for limiting passwords only for call records. The issues are much broader than the publicized issue of pretexting and the FCC should reject simplistic notions that customers do not like passwords.¹¹ These contentions lack any empirical support. If carriers must authenticate a customer's identity to access one category of information in the customer's account, there is no reason why the other account information shouldn't be protected, as well. Similarly, there is no empirical data that customers make distinctions between call and non-call detail. The public interest strongly favors that all CPNI information is password

⁹ / Statement of Commissioner Michael J. Copps Approving in Part, Dissenting in Part, Re: CPNI Order.

¹⁰ / Statement of Commissioner Jonathan S. Adelstein Approving in Part, Dissenting in Part, Re: CPNI Order.

¹¹ / CPNI Order at 10-11.

protected. Non-call detail contains sensitive personal information, which is just as worthy for protection from those looking to obtain such information for improper purposes. To protect consumer, expanded password protection is appropriate for non-call detail.

VI. THE FCC SHOULD REQUIRE MOBILE COMMUNICATIONS DEVICE MANUFACTURERS AND CARRIERS TO OFFER A MEANS OR METHODS FOR DELETING PERSONAL OR SENSITIVE INFORMATION FROM COMMUNICATIONS EQUIPMENT

Consumer use of mobile communications devices means that CPNI is frequently entered and stored in mobile devices. At the same time, customers lose their mobile devices or trade them in. The goal of expanded consumer protection can fully be realized by requiring manufacturers to design products with features that allow customers to establish passwords for access and permit deletion in bulk of all CPNI from devices. In addition, the FCC should weigh and consider the feasibility and costs of whether carriers should offer consumers the ability to delete or transfer CPNI when new phones are purchased. The FCC should establish what charges, if any, are fair, just and reasonable for such an option. The FCC should assess whether such technology exists in one form or another and the cost supplying this technology to consumers as an option. The benefits may out way the costs.

VII. CONCLUSION

In view of the foregoing, Rate Counsel submits that the public interest requires that the FCC consider the following:

- require password protection for all CPNI, not just call detail,
- explore the need for and the appropriateness of audit trails,
- establish data retention periods, and
- establish appropriate protections for CPNI on mobile devices, including methods for password protection and deletion.

Respectfully submitted,

Ronald K. Chen, Esq.
Public Advocate of New Jersey

Kimberly K. Holmes, Esq.
Acting Rate Counsel

By: *Christopher J. White*

Christopher J. White, Esq.
Deputy Public Advocate
Division of Rate Counsel

Dated: July 9, 2007