

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

<b>In the Matter of</b>	)	
	)	
<b>Implementation of the Telecommunications Act of 1996:</b>	)	<b>CC Docket No. 96-115</b>
	)	
<b>Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information;</b>	)	
	)	
<b>Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information</b>	)	<b>RM-11277</b>
	)	

**NATIONAL TELECOMMUNICATIONS COOPERATIVE ASSOCIATION  
INITIAL COMMENTS**

The National Telecommunications Cooperative Association (NTCA)<sup>1</sup> hereby responds to the Federal Communications Commission's (FCC's or Commission's) Notice of Proposed Rulemaking (NPRM)<sup>2</sup> seeking comment on what additional steps, if any, the Commission should take to further protect the privacy of customer proprietary network information (CPNI). NTCA respectfully submits that additional CPNI rules are unnecessary. Carriers cannot completely protect against the illicit and illegal acts of an unrelated third party. Rather than imposing new

---

<sup>1</sup> NTCA is the premier industry association representing rural telecommunications providers. Established in 1954 by eight rural telephone companies, today NTCA represents 560 rural rate-of-return regulated incumbent local exchange carriers (ILECs). All of its members are full service local exchange carriers, and many members provide wireless, cable, Internet, satellite and long distance services to their communities. Each member is a "rural telephone company" as defined in the Communications Act of 1934, as amended (Act). NTCA members are dedicated to providing competitive modern telecommunications services and ensuring the economic future of their rural communities.

<sup>2</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information* CC Docket No. 96-116; *Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, RM-11277, Notice of Proposed Rulemaking, FCC 06-10 (released Feb. 14, 2006).

and costly safeguards, the Commission should concentrate its efforts on working with carriers, the Federal Trade Commission (FTC) and law enforcement to identify and punish the wrongdoers. If the Commission determines that it must adopt stricter safeguards, it should recognize the limited resources of smaller carriers and permit maximum flexibility in compliance.

This proceeding was initiated as a result of a petition filed by the Electronic Privacy Information Center (EPIC).<sup>3</sup> EPIC asks the Commission to establish more stringent security standards for telecommunications carriers to govern the disclosure of CPNI. EPIC claims that numerous online data brokers and private investigators widely advertise their ability to obtain CPNI without the account holder's knowledge and consent. The NPRM proposes a number of additional security measures, some that would be quite costly and burdensome in their implementation, designed to remedy the problem. However, neither EPIC nor the FCC claims to know how these online data brokers and private investigators are obtaining unauthorized access to CPNI. It is therefore difficult, if not impossible to know if any of the proposed security measures will accomplish the stated goal. It is likely that whatever new measures the Commission adopts will be either under-inclusive or over-inclusive.

It is widely understood that the culprits obtaining and misusing CPNI are the data brokers. Although it is not fully known how they go about obtaining information, many suggest that it is by suspect means. The Commission discusses the possible use of "pretexting" which occurs when a person falsely represents that he or she is a company employee or a particular customer who seeks access to his or her own CPNI. Other possibilities include the "hacking" of

---

<sup>3</sup> Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) (EPIC Petition).

computer files, or dishonest insiders working for the carriers. The problems identified in the NPRM are not unique to the telecommunications industry. Any industry dealing with sensitive, individualized information struggles to keep its information and systems secure. No matter what security measures are employed, persistent wrong doers will eventually figure out how to bypass the systems and employ new ways to obtain information. The industry is asked to comment on proposals that will force it to spend millions of dollars to address the illegal and improper actions of a party over which it has no control. Current CPNI rules are designed to prevent carriers from misusing the CPNI of their own customers. The Commission now seeks to expand the obligation to prevent misuse by any party. If the Commission continues down this road, the industry will comment on a new CPNI proposed rulemaking every few years. Rather than impose new, costly security measures, the Commission should work with carriers, the FTC and law enforcement to identify wrong-doers. Only enforcement and the threat of future enforcement actions will deter parties from using illegal means to obtain information.

If the Commission determines that additional carrier security measures are necessary to protect customer CPNI, the Commission must take care to accommodate the interests of small carriers, including NTCA member rural telephone companies in accordance with the Regulatory Flexibility Act.<sup>4</sup> The financial and human resources of these small companies are limited.<sup>5</sup> The Commission must take care to avoid imposing overly burdensome and unnecessary expenses on rural carriers. Required security measures such as the encryption of computer records or

---

<sup>4</sup>The Regulatory Flexibility Act of 1980, as amended, requires that the Commission consider less burdensome CPNI regulations for small companies. 5 U.S.C. § 603, as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No 104-121 (1996).

<sup>5</sup> NTCA's members' customer bases range from less than 100 to more than 50,000. One half of NTCA member companies have less than 2,500 subscribers. The vast majority of NTCA member companies have less than 20 employees. Several members have fewer than 10 employees.

maintaining detailed audit trails will impose a cost that far exceeds the potential benefit. It is unclear how encryption or audit trails will deter data brokers, yet the expense is great.

Any new requirements should be minimally invasive, requiring no more than verification from the customer that a release of information is authorized.<sup>6</sup> Verification could be in the form of a customer-set password, verifying information, such as pets' or mothers' maiden names, or a phone call from the carrier to the customer confirming that a release of information is authorized. Rather than strict rules, the Commission should leave it to each small carrier to determine the best and most appropriate verification method. A very small carrier may find that it is cost-effective for it to call each customer before it releases information, a larger company may determine that passwords are the most economical solution. The solution for one carrier is not the solution for all carriers and the Commission should recognize this fact and adopt very flexible rules, particularly for small carriers.

The Commission also seeks comment on whether it should require carriers to obtain opt-in, rather than opt-out, consent from a customer before disclosing that customer's CPNI to the carrier's joint venture partners or independent contractors that provide communications-related services. There is no evidence or allegation that the disclosure of information to joint venture partners or independent contractors is contributing to the breach of CPNI security. The sharing of information benefits the consumer in that allows carriers to identify appropriate service bundles. The bundling of services offers the consumer convenience and usually, a cost savings. The requiring of opt-in consent will stymie bundling efforts and frustrate consumers while doing little to protect the security of customer information.

This proceeding was initiated because of the actions of unscrupulous data brokers. The Commission should reject calls for it to adopt costly, unproven and unnecessary new safeguards. Rather than forcing the telecommunications industry to spend millions of dollars installing new systems and training new personnel, and perhaps passing the cost onto their consumers, the Commission should concentrate its efforts on working with carriers, the FTC and law enforcement to identify and punish the wrong-doers. Any new requirements should be minimally invasive and permit maximum flexibility in compliance.

Respectfully submitted,

NATIONAL TELECOMMUNICATIONS  
COOPERATIVE ASSOCIATION

By: /s/ Daniel Mitchell  
Daniel Mitchell

Jill Canfield

Its Attorneys

4121 Wilson Boulevard, 10<sup>th</sup> Floor  
Arlington, VA 22203  
(703) 351-2000

April 28, 2006

CERTIFICATE OF SERVICE

I, Gail Malloy, certify that a copy of the foregoing Initial Comments of the National Telecommunications Cooperative Association in CC Docket No. 96-115, FCC 06-10 was served on this 28th day of April 2006 by electronic mail to the following persons.

/s/ Gail Malloy

Gail Malloy

Chairman Kevin J. Martin  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW, Room 8-A201  
Washington, D.C. 20554  
[Kevin.Martin@fcc.gov](mailto:Kevin.Martin@fcc.gov)

Commissioner Deborah Taylor Tate  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW, Room 8-B115  
Washington, D.C. 20554  
[Deborah.Tate@fcc.gov](mailto:Deborah.Tate@fcc.gov)

Commissioner Michael J. Copps  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW, Room 8-A302  
Washington, D.C. 20554  
[Michael.Copps@fcc.gov](mailto:Michael.Copps@fcc.gov)

Commissioner Jonathan S. Adelstein  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW, Room 8-C302  
Washington, D.C. 20554  
[Jonathan.Adelstein@fcc.gov](mailto:Jonathan.Adelstein@fcc.gov)

Best Copy and Printing, Inc.  
445 12th Street, SW  
Room CY-B402  
Washington, D.C. 20554  
[fcc@bcpiweb.com](mailto:fcc@bcpiweb.com)

Janice Myles  
Competition Policy Division  
Wireline Competition Bureau  
Federal Communications Commission  
445 12th Street, SW, Room 5-C140  
Washington, D.C. 20554  
[Janice.Myles@fcc.gov](mailto:Janice.Myles@fcc.gov)