

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)	RM-11277
)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information)	

REPLY COMMENTS OF CTIA–THE WIRELESS ASSOCIATION®

CTIA – The Wireless Association® (“CTIA”)¹ respectfully submits these reply comments in response to the Commission’s *Notice of Proposed Rulemaking* to enhance security and authentication standards for access to Customer Proprietary Network Information (“CPNI”).² CTIA and its members fully share the goal of protecting customer privacy and deterring data brokers from fraudulently obtaining calling records.

¹ CTIA is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the association covers Commercial Mobile Radio Service (“CMRS”) providers and manufacturers, including cellular, broadband PCS and ESMR, as well as providers and manufacturers of wireless data services and products.

² *In re* Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, *Notice of Proposed Rulemaking*, CC Docket No. 96-115, RM-11277 (Feb. 14, 2006) (“NPRM”); Wireline Competition Bureau Grants Request for Extension of Time to File Reply Comments in Response to the Commission’s Notice of Proposed Rulemaking to Enhance Security and Authentication Standards for Access to CPNI, *Public Notice*, CC Docket No. 96-115, DA 06-1033 (May 15, 2006).

EPIC's suggestion that the problem stems from lax carrier security rather than criminal acts of third parties is false. However well-meaning they might be, the proposed prescriptive regulations on carriers are not the optimal solution. Rather, reasonable and flexible oversight, such as clarification of the CPNI requirements and consumer education on security measures will help to prevent and deter pretexting. The competitive nature of the wireless industry necessitates that carriers provide excellent customer care and responsiveness, which includes safeguarding customer proprietary information. In order to achieve that goal, carriers and the Commission must balance the need to defend against fraudulent account access with customers' need for convenient access to their own account information.³

The Commission should recognize that carriers need flexibility to adopt new methods to combat fraudulent account access, and accordingly should allow carriers to determine the best ways to protect against unauthorized access of CPNI. While CTIA shares and supports EPIC's goals, the Commission should not mandate EPIC's proposals because they increase the regulatory burden for carriers with little, if any, benefit to consumers. Instead, the Commission should recognize carriers that establish best practice procedures, and provide these carriers a safe harbor from enforcement action. As CTIA noted in its initial Comments, CTIA also supports annual reporting requirements for carriers, and providing customers the option of further protecting their account information through password protection.

I. Wireless Carriers Are Committed To Protecting CPNI And Any Additional Security Measures Placed On Carriers Should Be Limited And Reasonable

³ See Comments of Alltel Corporation, CC Docket No. 96-115, RM-11277, at 3 (Apr. 28, 2006) ("Alltel Comments").

Wireless carriers are dedicated to safeguarding CPNI from disclosure to unauthorized parties. Not only do carriers have the duty to protect CPNI under the Commission's existing rules and Section 222 of the Communications Act, but carriers have a strong incentive to implement effective internal safeguards because the failure to do so would jeopardize customer retention.⁴ Wireless carriers have implemented internal mechanisms, including extensive employee training programs and dedicated financial and human resources, and continually are improving their security protocols.⁵ Moreover, carriers aggressively have pursued legal action against data brokers and actively support federal legislation aimed at imposing criminal sanctions on the wrongdoers themselves.⁶

CTIA and its members share EPIC's concerns about the pretexting problem. However, because the security problems arise from criminal acts of third parties, the prescriptive regulations EPIC recommends to be imposed on carriers are not the optimal solution. Rather, reasonable and flexible oversight, such as clarification of the CPNI requirements, adoption of the proposals CTIA made in its Comments,⁷ and consumer education on security measures will help to prevent and deter pretexting.⁸ If the Commission determines that new regulations are warranted, CTIA urges the Commission not to impose unnecessary, unduly costly, or overly burdensome regulations on carriers.

⁴ See Comments of Verizon Wireless, CC Docket No. 96-115, RM-11277, at 3 (April 28, 2006) ("Verizon Comments").

⁵ See Comments of Cingular Wireless LLC, CC Docket No. 96-115, RM-11277, at 4-6 (Apr. 28, 2006) ("Cingular Comments").

⁶ See Comments of T-Mobile USA, Inc., CC Docket No. 96-115, RM-11277, at 5-7 (April 28, 2006) ("T-Mobile Comments"); Comments of Sprint Nextel Corporation, CC Docket No. 96-115, RM-11277, at 7-9 (Apr. 28, 2006) ("Sprint Nextel Comments").

⁷ CTIA-The Wireless Association Comments, CC Docket No. 96-115, RM-11277 (May 1, 2006) ("CTIA Comments").

⁸ See *id.* at 8-9.

II. EPIC's Proposals Do Not Address The Identified Problem

CTIA cautions against the adoption of the rules proposed in the EPIC petition.⁹ Instead of punishing data brokers, the proposed rules are misdirected toward carriers by adding costs and burdens on carriers and their customers without effectively improving data security. If the Commission finds it necessary to adopt additional regulations, CTIA recommends narrowly targeted requirements that are measured and responsive to the actual problem presented.

A. The Commission Should Require That All Carriers Give Customers The Option Of Using Passwords For Account Access

CTIA supports a requirement that carriers give customers the option of using passcodes. Specifically, EPIC proposes that the Commission make consumer-set passwords mandatory to protect CPNI.¹⁰ Many carriers already offer password protection, especially for online account access, for those customers who seek extra protection beyond the typical verification procedures.¹¹ CTIA agrees that passcode protection is a valuable tool to deter fraud. Nonetheless, the Commission must consider its limitations since passwords are not completely effective or desired by every customer. Surveys have shown that some customers are burdened by having to remember numerous passwords for various accounts that may easily be forgotten or lost, and thus resist password protection for access to their account. In addition, there are customers who freely share their passwords with significant others and family members, therefore

⁹ Electronic Privacy Information Center Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115, RM-11277 (Aug. 30, 2005) (“EPIC Petition”).

¹⁰ *NPRM* at ¶¶ 15-16.

¹¹ *See* Verizon Comments at 8-9; T-Mobile Comments at 11; Alltel Comments at 4.

compromising the security of their own accounts.¹² As an alternative to forcing password usage for all account access, CTIA supports a requirement that carriers make passwords available to all customers for account access. Customers should then be informed of the benefits of such passwords and the ways to effectively safeguard account access.

B. CTIA Does Not Support An Opt-In Requirement For CPNI Disclosure To Carriers' Joint Venture Partners And Independent Contractors

With regard to CPNI disclosed to carriers' joint venture partners and independent contractors, the Commission asks whether requiring opt-in consent prior to disclosure would better protect CPNI notwithstanding the Commission's current safeguards or total service approach.¹³ Under the Commission's total service approach, carriers must obtain customers' consent through opt-out procedures prior to using CPNI to market services outside the customer's existing service.¹⁴ However, there is no evidence of data brokers obtaining CPNI through joint venture partners or independent contractors. Furthermore, these third parties typically do not have the access to the type of information that pretexters seek. Requiring customers to opt-in versus opt-out of shared communications will not increase protection because the problem does not lie with joint venture partners

¹² See Sprint Nextel Comments at 10-11; CTIA Comments at 13. These family members and significant others are precisely the types of persons who might be interested in obtaining access to account records for extra-judicial discovery in matrimonial and other domestic matters.

¹³ *NPRM* at ¶ 12.

¹⁴ *In re* Implementation of Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting; Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended, *Second Report And Order And Further Notice Of Proposed Rulemaking*, 13 FCC Rcd. 8061 (1998).

or independent contractors having access to CPNI, but rather the fraudulent acts of data brokers.¹⁵

C. The Burdens Imposed By Audit Trails Outweigh The Benefits

The *NPRM* seeks comment on whether to require an audit trail to record all instances of when a customer's records have been accessed, whether information was disclosed, and to whom.¹⁶ Routinely, carriers receive hundreds of thousands of customer service calls per day, which require access to CPNI to adequately answer customer questions.¹⁷ Depending upon the nature of the call, carriers will often electronically record the service request. However, logging all accesses and disclosures would impose a tremendous burden on carriers that would increase call time and add significant costs to generate such massive data storage.¹⁸ In this case, the Commission should follow its previous decision to repeal an audit trail requirement because audits trails would not sufficiently increase security to justify the costs and burdens imposed on carriers and customers.¹⁹

D. Encryption Will Not Obviate The Pretexting Problem

In its Petition, EPIC recommends that carriers be required to encrypt all stored CPNI data.²⁰ Thus far, the record shows no evidence of unauthorized access of stored

¹⁵ See Verizon Wireless Comments at 9-12.

¹⁶ *NPRM* at ¶¶ 17-18.

¹⁷ See Cingular Comments at 22.

¹⁸ See T-Mobile Comments at 15-16.

¹⁹ Telecommunications Carriers' Use of Proprietary Network Information and Other Customer Information, *Order on Reconsideration and Petitions for Forbearance*, 14 FCC Rcd 14409 (1999).

²⁰ *NPRM* at ¶ 19.

CPNI within carriers' databases.²¹ Encryption is already used to send customer records to outside sources such as credit bureaus but the issue here is not "hacking" or data brokers obtaining customer information by intercepting transmission of data to third party affiliates. The concern is pretexting where records have to be accessed by authorized personnel and disclosed in unencrypted form to the customer. As a result, encryption of stored call records would have no effect of preventing pretexting, but would increase costs, potentially delay response to legitimate customer service inquiries, and complicate carrier storage and access methods.²²

E. The Commission Should Not Adopt New Notice Requirements

The Commission should not adopt EPIC's proposals to implement rules requiring carriers to notify customers when the security of CPNI may have been breached.²³ With the greater percentage of legitimate customer service calls requiring access to CPNI, compared to the small number of fraudulent pretexting calls, advance notice would be inconvenient and expensive, and would unreasonably impede carriers' ability to provide prompt customer service. Further, post-disclosure of CPNI would generate confusion and unnecessary concern among customers who do not recall communicating with their wireless customer service representative or otherwise condition customers to ignore the notifications as routine.²⁴

F. Limiting Data Retention Is Ineffective In Protecting CPNI

²¹ See Verizon Wireless Comments at 15; Sprint Nextel Comments at 14.

²² See CTIA Comments at 15.

²³ See EPIC Petition at 11.

²⁴ See Cingular Comments at 25-26; CTIA Comments at 17-18.

CTIA believes that limiting data retention would not remedy the pretexting problem. Carriers' data storage policies result from a number of reasons, including dispute resolution over wireless charges and documenting past events for law enforcement and litigation matters. Due to the costs associated with data storage and retrieval, carriers are inclined to maintain call records for no longer than necessary. Although, some carriers may not be opposed to shortening retention periods, it is impractical given the need to utilize the records for various purposes.²⁵

III. CTIA Believes The Commission Can Take Some Positive Steps To Help Prevent And Deter Pretexting

CTIA supports the Commission's actions to address the authorized disclosure of CPNI. Carriers aim to provide the utmost protection of customer's private information without compromising the quality of the customer experience. Any regulations adopted in this proceeding, must allow carriers the flexibility to respond to customer needs while guarding customer data. CTIA agrees that greater transparency is needed with regard to carriers' CPNI certifications to the Commission, including representations that the carrier has implemented security procedures and conducted privacy training for employees.²⁶ Also, carriers willing to take affirmative steps to prevent pretexting should be afforded safe harbor protections against enforcement action. Similar to the safe harbor policy for do-not-call rules,²⁷ CTIA agrees that the Commission should establish voluntary standards that carriers could comply with to avoid liability.²⁸ Furthermore, carriers should maintain and inform customers of their privacy policies by alerting customers of

²⁵ See Cingular Comments at 24-25.

²⁶ See CTIA Comments at 2-3.

²⁷ 47 C.F.R. § 64.1200(c)(i).

²⁸ See Verizon Wireless Comments at 21.

how their information is collected and used as well as what steps the customer can take to protect personal information.

IV. Conclusion

CTIA and its members share the Commission's concern for the confidentiality of CPNI. While carriers are constantly improving their complex security procedures and protocols, carriers must preserve the customer experience, including giving customers control over their accounts. CTIA urges the Commission to deny EPIC's proposals because they are overly burdensome for carriers with little potential to improve security. If the Commission determines that added regulations are necessary, any new regulations must be cost effective and narrowly tailored to deter and prevent pretexting.

Respectfully submitted,

/s/ Marlo A. Go

Marlo A. Go
Staff Counsel

Michael F. Altschul
Senior Vice President & General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

CTIA – THE WIRELESS
ASSOCIATION®
1400 16th Street, N.W., Suite 600
Washington, D.C. 20036
(202) 785-0081

June 2, 2006