

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)	
)	

To: The Commission

CTIA – THE WIRELESS ASSOCIATION® COMMENTS

Michael F. Altschul
Senior Vice President & General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Paul Garnett
Assistant Vice President, Regulatory Affairs

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

SUMMARY

CTIA – The Wireless Association® wholeheartedly supports the Commission’s goal of protecting carriers and customers from data brokers fraudulently obtaining calling records by impersonating a legitimate carrier customer. In the competitive wireless industry, carriers have every incentive to protect the records of their customers. CTIA’s members have taken many steps to prevent or deter pretexting fraud. However, no combination of safeguards will entirely protect against individuals intent on defrauding carriers and their customers. CTIA supports steps that will advance the shared goal of protecting customer privacy and deterring pretexting. CTIA supports:

- A requirement that all carriers make passwords available to all customers for account access.
- An amendment to Section 64.2009 requiring that each carrier’s annual Customer Proprietary Network Information (“CPNI”) certification be filed with the Commission and include representations that the carrier has implemented security procedures to prevent unauthorized CPNI disclosures and conducted privacy and security training during the prior year for those personnel who have access to CPNI.
- A rule prohibiting disclosure of a customer’s Social Security number (“SSN”), Taxpayer Identification number, credit card number, or billing name and address in response to inbound customer calls.
- A requirement that carriers publish their privacy policies to inform consumers of the availability of password protection and other security measures.

CTIA does not support the adoption of specific and prescriptive security procedures. Such an approach would be counterproductive and, in some cases, provide a roadmap to circumvent security. This proceeding also should not be used to create CPNI procedures unrelated to the pretexting problem, such as customer opt-in for all access, use, and disclosure of CPNI. Instead, CTIA’s proposals are measured and responsive to the actual problem presented.

TABLE OF CONTENTS

I.	DISCUSSION	4
A.	The Nature and Scope of the Problem	5
B.	Commission Intervention	8
C.	Wireless Carrier CPNI Security Practices.....	12
D.	EPIC’S Additional Security Elements	13
(1)	Consumer-Set Passwords	13
(2)	Audit Trails.....	14
(3)	Encryption	15
(4)	Limiting Data Retention	15
(5)	Notification.....	16
II.	CONCLUSION	19

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)	
)	

To: The Commission

CTIA – THE WIRELESS ASSOCIATION® COMMENTS

In response to a petition filed by the Electronic Privacy Information Center (“EPIC”) requesting a rulemaking to require carriers to institute more stringent security measures to protect against the unauthorized release of customer calling records,¹ the Federal Communications Commission (“Commission”) seeks comment “on what additional steps, if any, the Commission should take beyond existing rules to protect the privacy of customer proprietary network information (“CPNI”) that is collected and held by telecommunications

¹ 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”); *In re* Petition of Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, *Public Notice*, Report No. 2726, RM-11277 (Sept. 29, 2005).

carriers.”² CTIA – The Wireless Association®³ (“CTIA”) supports the Commission’s inquiry and fully supports the goal of protecting carriers and customers from the alleged ability of third party data brokers to obtain calling records by impersonating a legitimate carrier customer or using other fraudulent tactics.⁴ In the competitive wireless industry, carriers have every incentive to protect the records of their customers. CTIA’s members have taken many steps to prevent or deter pretexting fraud. In these comments, CTIA proposes some additional steps that will advance the shared goal of protecting customer privacy.

Specifically, CTIA supports a requirement that all carriers make passwords available to all customers for account access. Customers should be informed of the benefits of using such passwords and customers should be given an opportunity to use a password of their choosing to safeguard access to their account. CTIA believes that customer-set passwords will reduce the opportunity for fraud. Because passwords may be forgotten or lost, carriers should be afforded the latitude to employ best practices when resetting a customer’s password.

Further, CTIA supports greater transparency in carrier certifications regarding CPNI protection. To that end, CTIA supports amendment of Section 64.2009 to require that each

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, ¶ 1 (Feb. 14, 2006) (“NPRM”).

³ CTIA - The Wireless Association® is an international organization representing all sectors of wireless communications – cellular, personal communication services, and enhanced specialized mobile radio.

⁴ Such illicit tactics are a form of identity theft and commonly are referred to as “pretexting.”

carrier's annual CPNI certification be filed with the Commission and include representations that the carrier has implemented security procedures to prevent unauthorized CPNI disclosures and conducted privacy and security training during the prior year for those personnel who have access to CPNI.

Next, while many carriers already have implemented this procedure, CTIA believes a rule that prohibits disclosure of a customer's Social Security Number, Tax ID, credit card number or billing name and address in response to inbound customer calls would be prudent.⁵ While some customers may be inconvenienced by this rule, it is a common pretexting tactic to call carriers and pretend to be a relative, employer, or other "authorized" person needing access to such information for an emergency.

Additionally, carriers can and should convey these measures in their privacy policies. CTIA's Consumer Code for Wireless Service⁶ already requires carriers to adopt privacy policies, and this requirement could be incorporated into these privacy policies. CTIA does not support the adoption of specific and prescriptive security procedures. Such an approach would provide a roadmap to circumvent security. Instead, CTIA's proposals are measured and responsive to the actual problem presented. Unfortunately, in comparison, many of the proposals set forth by EPIC in its petition will do nothing to protect against the unauthorized

⁵ CTIA's proposal would not prohibit disclosure of the last four digits of a customer's SSN, Tax ID, or credit card number. Limited disclosure of these digits is often used to assist customers with validating their account information, but by itself, does not permit misuse of this information.

⁶ CTIA Consumer Code for Wireless Service, at http://files.ctia.org/pdf/The_Code.pdf.

release of customer calling records, and CTIA explains below why the Commission should reject those ideas.

I. DISCUSSION

In the NPRM, the Commission specifically requests comment on the issues raised by EPIC in its petition. EPIC initially petitioned the Federal Trade Commission (“FTC”) on July 7, 2005, to inquire into the deceptive and fraudulent practices of online information brokers who purported to offer subscriber telephone records for sale.⁷ EPIC then petitioned the Commission on August 30, 2005, to initiate a rulemaking to require carriers to institute more stringent security measures to protect against the unauthorized release of customer calling records to these information brokers.⁸ CTIA and others provided extensive comments to the Commission at that time and called for increased enforcement of the existing laws against such data brokers.

Because the pretexting problem has become so publicized, and in response to the perceived ease with which records have reportedly been obtained, the Commission now seeks comment on three distinct issues: (1) the nature and scope of the problem identified by EPIC; (2) whether Commission intervention will adequately solve the problem; and (3) the nature of carrier practices in regard to safeguarding CPNI.⁹ The Commission also seeks

⁷ See *In re Intelligent e-Commerce, Inc., Complaint and Request for Injunction, Investigation and for Other Relief* (July 7, 2005).

⁸ See EPIC Petition.

⁹ See NPRM at ¶¶ 11-13.

comment on the advisability and feasibility of implementing EPIC's five proposed security measures.¹⁰ CTIA addresses the Commission's questions first and then responds to EPIC's proposals.

A. The Nature and Scope of the Problem

The Commission asks for more detail about the nature and scope of the pretexting problem. Online brokerage of call records is just a new marketing twist for an old fraud profession. As the Commission knows, on February 1, 2006, Congress held its first hearing on the cell phone pretexting issue.¹¹ CTIA President and Chief Executive Officer Steve Largent testified at that hearing about wireless carriers' experience with pretexting:

Make no mistake, these data thieves are extremely sophisticated. If they are unable to deceive one CSR on the first attempt, they will place multiple calls to customer service call centers until they are able to mislead a CSR into providing the call records.

No combination of identifiers is safe against pretexting. We have had cases where the data brokers have possessed the customer password. We have had cases where they knew the date of birth of the customer and the full Social Security number.¹²

Robert Douglas, an information security consultant, echoed Mr. Largent's testimony, providing a succinct statement of how pretexting occurs:

¹⁰ See *id.* at ¶ 14.

¹¹ See Hearing on "Phone Records for Sale: Why Aren't Phone Records Safe from Pretexting?" Before the U.S. House of Representatives Committee on Energy & Commerce, (Feb. 1, 2006) ("Pretexting Hearing").

¹² See *Pretexting Hearing*, Prepared Statement of Steve Largent at 3.

To further understand pretexting you need to know the code of the identity thief, broker, or investigator seeking information they don't have legitimate access to.

- 1) Know what piece of information you want.
- 2) Know who the custodian of the information is.
- 3) Know who the custodian will release the information to.
- 4) Know under what circumstances the custodian will release the information.
- 5) Become that person with those circumstances.

Once you know the code and apply a little imagination and bravado, you can steal almost any piece of information in this country.¹³

While the anatomy of the pretexter is interesting, the point that cannot be over-emphasized is that by the time the pretexter has obtained enough information to contact the carrier, to the carrier, the pretexter is the customer. And as Mr. Douglas suggests, prescriptive rules detailing specific security practices that must be followed by all carriers do nothing more than provide a road map to criminals and erect a barrier that prevents carriers from adopting new security measures in response to constantly evolving threats from data thieves who become more knowledgeable with every call to a carrier's customer service representatives.

Who are these criminals? Mr. Douglas aptly pointed out the salient fact that it is the market makers that create the incentives for pretexting fraud – attorneys, private investigators,

¹³ *Pretexting Hearing*, Prepared Statement of R. Douglas at 4.

and others who seek call records for their own investigative or malicious reasons.¹⁴ While the theft of a customer's phone records is an invasion of the customer's privacy, it is not identity theft because all of the data needed to steal that customer's identity is in the hands of the pretexter before the call is made to the carrier; often this identity information is for sale online by these same brokers. CTIA urges the law enforcement community and agencies to focus on the market makers to make a real impact on the pretexting problem by drying up the demand for obtaining call records through pretexting and other false premises.¹⁵

To that end, the FTC is investigating companies that offer consumer telephone records for sale and plans "to pursue these investigations vigorously."¹⁶ In addition, Chairman Barton's Committee has issued subpoenas to a dozen information brokers seeking among other things, records related to who bought call records, who provided them, and how

¹⁴ *Id.* at 6-7. Many of the persons who purchase call records are regulated and licensed professionals. Soliciting another person to obtain call records through pretexting is actionable, and these professionals ought to be subject to ethical or licensure restrictions. CTIA urges the state attorneys general, professional standards and accreditation groups, and others to vigorously investigate and sanction any professional who is responsible for purchasing call records through a data broker or any other person who obtains this information through pretexting or other fraudulent means.

¹⁵ For all the discussion and hearings, the scope of the pretexting problem remains largely unknown. While publicity surrounding the issue highlighted the apparent ease of obtaining records through online data brokers, this is misleading. The fact that call records *could* be acquired through data brokers does not mean that *it was being done* on any large scale. Because the service is expensive – in some cases hundreds of dollars for a single call record – it is doubtful that call records were common currency. But unless future discovery or compulsion yields up the records from these data brokers, to the extent they maintained any, the Commission will not know how big the actual market was or is for these illicit services.

¹⁶ See Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation Subcommittee on Consumer Affairs, Product Safety, and Insurance, U.S. Senate (Feb. 8, 2006).

it was done.¹⁷ Thus the scope of the pretexting problem may become better known and understood sooner rather than later.

B. Commission Intervention

The Commission asks whether its intervention by the promulgation of new rules will solve the problem of pretexting. The question is a fair one, and CTIA appreciates that the Commission has asked it rather than simply reacting to headlines and proposing rules. First, CTIA rejects EPIC's suggestion that the problem with pretexting lies with lax carrier security rather than with the criminal acts of third parties. The Commission's own inquiry process should make clear that carriers have not knowingly released information to anyone other than the supposed customer.¹⁸ However, as noted at the outset, CTIA believes the Commission can take some positive steps to help prevent and deter pretexting.

Specifically, CTIA supports a requirement that all carriers make passwords available to all customers for account access. We discuss this proposed requirement in more detail below in response to the EPIC password proposal and the Commission's specific request for

¹⁷ See News Release, U.S. House of Representatives Committee on Energy & Commerce, Committee Subpoenas Companies Claiming to Sell Private Phone Records, at http://energycommerce.house.gov/108/News/04062006_1844.htm.

¹⁸ EPIC itself admits that by the time the request is made to the carrier for call records, the fraudster already has acquired the customer's date of birth, mother's maiden name or social security number or other identifiers from databases, public records or other sources on the Internet. See EPIC Petition at 8, 11. In other words, the requesting party in all respects appears to be the customer. While a rule may outlaw fraud, it cannot prevent it from happening. Even if the customer was required to appear in person at a carrier retail store with government issued identification, false credentials may be used to circumvent the safeguard. Commission intervention will not solve this conundrum.

comment.¹⁹ As a general proposition, customers should be informed of the benefits of using such passwords and be given the choice to do so. CTIA acknowledges that customer-set passwords likely will reduce the opportunity for fraud. While passwords may be forgotten or lost, as CTIA noted in prior comments,²⁰ carriers will employ best practices when resetting the password if necessary, and it may be that the initial deterrent of a password protected account is enough to deter at least the casual fraud.

Further, CTIA supports greater transparency in carrier certifications regarding CPNI protection. To that end, CTIA supports the Commission's proposed amendment of Section 64.2009(e) to require that the annual CPNI certification be filed with the Commission.²¹ CTIA also suggests that the certification include representations that the carrier has implemented security procedures to prevent unauthorized CPNI disclosures and conducted privacy and security training during the prior year for those personnel who have access to CPNI.

The Commission further proposes to require carriers to report "any actions taken against data brokers and a summary of all consumer complaints received in the past year concerning the unauthorized release of CPNI."²² Read broadly, this proposal would impose massive costs on carriers with only limited benefits. First, it is unclear what the Commission

¹⁹ See NPRM at ¶¶ 15-16.

²⁰ See CTIA-The Wireless Association®, Comments in Opposition to Epic Petition For Rulemaking, CC Docket No. 96-115, RM-11277, at 18 (Oct. 31, 2005).

²¹ See NPRM at ¶ 29.

²² *Id.*

means by “any action.” An action might include an investigation, a cease and desist letter, a referral to the FTC or law enforcement, or a lawsuit. CTIA respectfully suggests that such reporting would be counterproductive, would potentially invade attorney-client privileges and the work product privilege, and would disclose information that otherwise may hinder an investigation. Moreover, the current trend suggests that carrier actions have had their impact and that future legislation and consumer protection initiatives may shift the legal action to law enforcement or consumer protection agencies.

Second, because customers contact carriers through many different avenues (including walking in to a carrier’s retail outlet, casually stopping by an agent’s kiosk in a mall, and by calling customer care) there is no centralized system to capture and categorize complaints to adequately meet the proposed requirement. Because pretexting is a crime of stealth, customer and carrier alike generally are unaware of it, and carriers have received virtually no notice, or complaints from customers regarding unauthorized release of information. CTIA believes the proposed requirement would place a huge burden on carriers to develop systems to manage complaints that may never come.

Moreover, the Commission already maintains an effective consumer complaint process. The Commission’s Consumer Inquiries and Complaints Division receives, reviews, and analyzes consumer complaints. In addition, the Commission publishes a quarterly report of consumer inquiries and complaints.²³ While these reports have never noted any consumer

²³ Federal Communications Commission, Quarterly Inquires and Complaints Reports, *at* <http://www.fcc.gov/cgb/quarter/welcome.html>.

inquiries or complaints regarding the unauthorized disclosure of CPNI, the Commission's own data is the best and most reliable mechanism for tracking consumer concerns.

Next, while many carriers already have implemented this procedure, CTIA supports the creation of a baseline rule that prohibits disclosure of a customer's Social Security Number or credit card number (other than the last four digits of a credit card), Tax ID, or billing name and address in response to inbound customer calls. The real customer would possess this information already.

Carriers receive pretexting calls from putative relatives, employers, or other "authorized" persons requesting access to such information for an emergency, because the customer is incapacitated or in the hospital, or in order to pay a bill. While this rule may create some inconveniences for real customers, it is far more likely to deter pretexting.

Finally, carriers can and should use their privacy policies to convey to their customers the security protections that are available to safeguard account information. CTIA's Consumer Code for Wireless Service already urges carriers to adopt and post privacy policies to explain information practices, and the Commission could incorporate this requirement in its rules.²⁴ In doing so, the Commission could require that the above security measures be explained in such a policy. Put another way, an online privacy policy is an education vehicle for customers – explaining that passwords are important to protect against pretexting and that customers should keep their password confidential.

²⁴ See CTIA Consumer Code for Wireless Service, at http://files.ctia.org/pdf/The_Code.pdf.

C. Wireless Carrier CPNI Security Practices

In response to its Letters of Inquiry, the Commission no doubt has received detailed explanations of wireless carriers' procedures to safeguard CPNI. There has been no suggestion in the public record that the CPNI rules are inadequate for their original purpose – the regulation and control of the use of CPNI for marketing by carriers. This proceeding should not be used as an excuse to require, for example, customer opt-in for all access, use, and disclosure of CPNI.

To the contrary, most wireless carriers do not disclose CPNI to third parties or use it outside the total service approach. This means that the risk of unauthorized disclosure actually is less than EPIC perceives under existing CPNI rules. When third parties have access to CPNI to perform some function such as billing, as required by the Commission's rules, the access is made pursuant to confidentiality agreements. The record is completely devoid of any evidence that carrier marketing practices are responsible for any pretexting disclosures.

Accordingly, in response to the Commission's specific question, CTIA believes the existing opt-out regime for marketing adequately protects the privacy of CPNI and no changes are necessary or desirable.²⁵

²⁵ NPRM at ¶ 12.

D. EPIC's Additional Security Elements

(1) Consumer-Set Passwords

The Commission asks whether a customer-set password would materially increase the security of CPNI.²⁶ CTIA acknowledges that use of customer-set passwords for account access could reduce the risk of fraudulent access. Accordingly, CTIA would support a rule that required carriers to make such a password available to customers and to provide a notice to customers of the importance of using and safeguarding such passwords for account access, but CTIA does not support mandating passwords. Customers should be free to choose, as long as they are informed of the risks.

If the Commission adopts a rule that requires carriers to provide customers with the option of securing their account data with a password of their choosing, the Commission should limit such a rule to account access to CPNI and provide a reasonable period of time for all carriers to implement a password system. The Commission should also create a safe harbor for carriers that disclose account information to any person who provides a correct password.

Because customers forget or lose passwords, carriers will need to reset lost or stolen passwords or administratively reset a password when necessary. CTIA does not propose to specify the manner or means of accomplishing a reset on the record. Carriers will employ best practices to accomplish the reset and to notify the customer of the change. At a minimum, however, CTIA agrees that password changes and notification should not and will not occur in the same inbound customer call that reports the loss.

²⁶ NPRM at ¶¶ 15-16.

(2) *Audit Trails*

EPIC further calls for audit trails regarding access to CPNI. The Commission asks for comment on whether Section 64.2009(c) requirements for recording use of CPNI in marketing campaigns should be extended to individual CPNI disclosures.²⁷

To point out the obvious - an audit trail is useful only once the disclosure is known to have occurred. The record should be clear on pretexting – to the extent that carriers may have disclosed CPNI, it was with the belief, based on identifying information provided by the requesting party, that CPNI was being disclosed to the customer. The audit trail is clear in these cases: customer service representatives' annotations note that such a disclosure was being made at the customer's request. CTIA fails to understand what new audit trail rules would achieve or how the forensic or audit capabilities of carriers are deficient in light of what already is known and well understood about how call records are obtained fraudulently through pretexting.

The Commission's Safeguard Rules require carriers to keep a record of CPNI accessed or used in marketing campaigns.²⁸ This is a vastly different requirement than individually recording each CPNI access made for any purpose, from troubleshooting to billing dispute, from emergency response to responding to lawful process, to customer requests by phone, email, or in writing for account balance information and billing inquiries. CTIA agrees with BellSouth's previous comments regarding the cost and maintenance of

²⁷ NPRM at ¶ 18.

²⁸ 47 C.F.R. § 64.2009(c).

such a system,²⁹ and we add that the development of an enterprise-wide audit function would not be trivial. In short, the benefits in preventing pretexting are small to nonexistent, and the burdens are great, especially when the existing methods have not been shown to be inadequate.

(3) Encryption

EPIC also calls for encryption of stored call records. The Commission asks whether encrypting stored CPNI would be useful and worth the cost.³⁰ The record here establishes that disclosure of call records to data brokers occurs by means of fraud, not by brute force or by hacking into carrier databases.

Moreover, encryption would do nothing to obviate the pretexting problem because, as CTIA pointed out in its comments, such records obviously would have to be accessed by authorized personnel and disclosed in unencrypted form to the customer. Encryption does nothing to protect the customer from being impersonated. Encryption will increase carrier expense, slow down customer service access to records in response to the overwhelming majority of legitimate inquiries received from customers, and vastly complicate carrier storage and access methods with no corresponding benefits. CTIA also notes that not even the security rules related to financial information require encryption for stored data.

(4) Limiting Data Retention

The Commission asks for further comment on EPIC's calls for the destruction of calling records when they are no longer needed for billing or dispute purposes or for removal

²⁹ See Opposition of BellSouth Corporation, RM-11277, at 5-6 (Oct. 31, 2005).

³⁰ NPRM at ¶ 19.

of personally identifying information from the records after some period of time. As CTIA pointed out in its comments, historical calling records serve many legitimate purposes, from assisting customers who need to validate their wireless charges and document past events to responding to legal process from law enforcement in criminal and national security matters. CTIA doubts that older records are the target of data brokers. Many carriers archive such records in any event, and it takes time to retrieve them upon request. Again, these records do not seem to be of interest to data brokers. In short, in the absence of a record to the contrary, the remedy has no relationship to the problem.

(5) Notification

EPIC suggests that carriers notify customers when the security of their CPNI has been breached. The Commission asks the right question instead – should carriers be required to notify customers before any disclosure of CPNI?³¹ As beguiling as routine notification might be, CTIA concludes that such notice would be ineffectual, annoying to customers and impractical.

First, as CTIA noted in its earlier comments, over 100 million customer service inquiries are received each year. Many of these requests necessitate access to CPNI to resolve a customer's concern. We do not know the total number of pretexting cases, but we do not believe that the number is large. We see no record of lawsuits, customer complaints, or governmental investigations of the practice before the recent publicity associated with and following the EPIC Petition. Accordingly, we believe the percentage of customer service calls constituting fraudulent pretexting to be small, especially compared to millions of

³¹ NPRM at ¶¶ 22-23.

customer service inquiries carriers receive each year. If that is true, requiring advance notice before disclosure of CPNI to the customer would result in significant inconvenience and delay in the vast number of legitimate requests.

Second, any requirement imposing a duty on carriers to notify customers in advance of releasing CPNI would need to specify how the carrier is expected to contact the customer. Calling or sending a text message to the wireless phone associated with the account may annoy legitimate customers, and certainly will frustrate those customers who do not have their phone with them; or customers who contact customer service regarding a spouse or child's handset that is billed to them; or customers who may be calling customer service on a wireline because the construction and location of their workplace doesn't enable in-building wireless service. Mail notification is much slower, and will needlessly frustrate legitimate callers. And if advance notice also requires acknowledgment by the customer of the request before call records can be released, what acknowledgment would the carrier expect in return? As noted above, no single method is fraud proof.³²

Post-CPNI disclosure notice might serve the purpose of an early alert to customers if CPNI was improperly released. But here again, the likely cost of notifying legitimate customers of routine and legitimate CPNI access or disclosure outweighs the benefit, even assuming notification was limited to contacts with customer service representatives (as opposed to database maintenance, billing analysis, marketing, etc.). Moreover, the customer

³² Even if carriers were to require every customer to appear in person at a carrier store and present a government issued identification card as a predicate to obtaining access to the customer's call records, is there any reason to believe fraudsters would be any more deterred than underage college students from counterfeiting identification cards in order to impersonate the customer?

confusion such disclosures predictably would generate with customers who did not remember contacting customer service, or who did not associate their contact with the need to access call records, would generate more calls to customer service, which in turn would generate additional disclosure notices and even more confusion and unwarranted concern.

II. CONCLUSION

CTIA and its members share the Commission's concern for the confidentiality of CPNI. CTIA members take security and privacy seriously and are committed to protecting customer information. While the Commission cannot codify perfect security, because such a thing does not exist, adopting CTIA's proposals should improve the security environment.

Finally, CTIA continues to support the strongest measures against those who traffic in personal information in unlawful or deceptive ways. Congress is considering laws to explicitly criminalize pretexting for call records today. The FTC continues its investigations and carriers are pursuing injunctive relief against known pretexters as well. CTIA welcomes efforts from the Commission – in line with these comments – as part of government's efforts to stop this deceptive practice.

DATED: May 1, 2006

Respectfully submitted,

/s/ Michael F. Altschul

Michael F. Altschul
Senior Vice President & General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Paul Garnett
Assistant Vice President, Regulatory Affairs

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