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

In the Matter of	)	
	)	
Electronic Privacy Information Center	)	
	)	CC Docket No. 96-115
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277

To: The Commission

CTIA – THE WIRELESS ASSOCIATION®
COMMENTS IN OPPOSITION TO EPIC PETITION FOR RULEMAKING

Michael F. Altschul
Senior Vice President, General Counsel

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

October 31, 2005

SUMMARY

On July 7, 2005, the Electronic Privacy Information Center ("EPIC") petitioned the Federal Trade Commission ("FTC") to inquire into the deceptive and fraudulent practices of online information brokers who purport to offer subscriber telephone records for sale. EPIC then petitioned the Federal Communications Commission ("Commission") to initiate a rulemaking to require telecommunications carriers to institute more stringent security measures to protect against the unauthorized release of customer proprietary network information ("CPNI") to these information brokers.

CTIA – The Wireless Association® ("CTIA") opposes the EPIC Petition because wireless carriers already take extraordinary steps to protect CPNI and existing Commission rules more than adequately CPNI security requirements. Moreover, legislation and rules create a comprehensive approach to privacy and security that encompasses CPNI within the enterprise. Additional rules aimed solely at CPNI therefore would be both duplicative and under-inclusive, yielding no consumer benefit while imposing unnecessary additional burdens on carriers.

Finally, the law is clear in regard to illegal access to CPNI. CTIA strongly supports enforcement of that law against information brokers or others who violate it. The FTC is best situated amongst the regulatory agencies with possible jurisdiction to investigate the practices of online information brokers who purport to offer customer calling records that could not otherwise be obtained without customer consent or valid legal process.

TABLE OF CONTENTS

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

In the Matter of	)	
	)	
Electronic Privacy Information Center	)	
	)	CC Docket No. 96-115
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277

To: The Commission

CTIA – THE WIRELESS ASSOCIATION®
COMMENTS IN OPPOSITION TO EPIC PETITION FOR RULEMAKING

On July 7, 2005, the Electronic Privacy Information Center ("EPIC") petitioned the Federal Trade Commission ("FTC") to inquire into the deceptive and fraudulent practices of online information brokers who purport to offer for sale, among other things, subscriber telephone records.[1] CTIA – The Wireless Association®[2] ("CTIA") fully supports the notion of holding information brokers accountable for their acquisition and sale of telephone records obtained by illegal and fraudulent means. The FTC has not yet acted on the petition.

[1] *See In the Matter of Intelligent e-Commerce, Inc.*, Complaint and Request for Injunction, Investigation and for Other Relief (July 7, 2005).

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

EPIC then petitioned the Federal Communications Commission ("Commission") to initiate a rulemaking to require telecommunications carriers to institute more stringent security measures to protect against the unauthorized release of customer proprietary network information ("CPNI") to these information brokers.[3] The EPIC Petition assumes incorrectly that such records may only be obtained through lax carrier security procedures. To the contrary, CTIA's members are committed to protecting customer privacy and security. Wireless carriers employ a broad range of security measures, even beyond those required in the Commission's CPNI Safeguards rule, to prevent unauthorized access to and disclosure of CPNI. To the extent CPNI is obtained under false pretenses, carriers are victims of a crime and are entitled to their remedies under the law. EPIC seemingly prefers to blame the victim for the unlawful acts of the criminal.

Further, EPIC requests the Commission to require carriers to identify their security procedures on the record and to actually identify the inadequacies in those procedures. The public record is no place to discuss those measures. At best, such an approach would be a further prescription for fraud.

Instead, CTIA supports vigorous enforcement of the law. Its members already are subject to a variety of laws that include security requirements, which we review below; and wireless customers have direct and powerful remedies in the event of any unauthorized disclosure of CPNI. The Commission should cooperate with the FTC in any investigation it chooses to undertake into the practices of information brokers,

---

[3] Electronic Privacy Information Center Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, *Consumer and Governmental Affairs Bureau Reference Information Center Petition for Rulemaking Filed*, RM-11277, *Public Notice*, Report No. 2726 (rel. Sept. 29, 2005)("EPIC Petition").

and any entity found to be violating the law should be punished. But EPIC's attempt to impose new security requirements on carriers – part of its larger agenda to do so across all entities – is misguided and misinformed and should be rejected.

I. WIRELESS CARRIER SECURITY PRACTICES

Wireless carriers take the security of their customers' information very seriously and have implemented security measures to protect against the unauthorized release of CPNI. Of course, no two carriers can or should employ the exact same security procedures,[4] but as a general proposition, wireless carriers all have security policies and employ security best practices. As noted at the outset of these comments, CTIA strongly disagrees with EPIC's request that the Commission require wireless carriers to identify security procedures on the record and to further identify any inadequacies in those procedures. Doing so would provide a roadmap to criminals to avoid fraud detection measures employed by carriers and could lead to serious harm to consumers and carriers alike.[5]

Instead, in the sections that follow, CTIA explains the general principles of security employed by carriers and the legal underpinnings of their security programs so that the Commission will understand that security is no second thought at wireless

---

[4] As a general proposition, robust security really cannot be codified in rules of general applicability. The threat environment is constantly changing and static rules quickly become outmoded.

[5] EPIC's request to identify the inadequacies in security procedures demonstrates the overall uninformed nature of the petition and the general lack of understanding about security practices. If security inadequacies were known or perceived, they would be corrected, not ignored. Security audits, training, and testing are ongoing activities at wireless carriers aimed at the continuous improvement of security in the face of continuous attempts to gain access to network facilities or to steal or disrupt services. Security is a way of life for every network operator today.

carriers. Indeed, in today's privacy sensitive times, security and privacy go hand in hand.

A. Wireless Carrier CPNI Practices

The heart of EPIC's Petition is the allegation that the Commission's CPNI rules are inadequate because they do not address in detail security measures EPIC believes necessary to protect CPNI from unauthorized disclosure to information brokers. While CTIA and EPIC agree on the importance of securing wireless customers' account data, the EPIC Petition reveals its ignorance about the Commission's rules and carrier CPNI practices.

CPNI is protected from unauthorized disclosure under Section 222 of Title 47 and the Commission's implementing rules.[6] "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information."[7] Every wireless carrier takes that duty seriously; it is the law.

Carriers are only permitted to disclose CPNI in a limited number of circumstances. First, a carrier is obligated to disclose CPNI to any other person on the customer's written authorization.[8] Further, carriers are permitted to access, use and disclose CPNI with the customer's prior oral or electronic approval;[9] to initiate,

---

[6] 47 C.F.R. §§ 64.2003 *et seq.*

[7] 47 U.S.C. § 222(a).

[8] 47 U.S.C. § 222(c)(2). Once CPNI is in the hands of a third party for any reason at the direction of a customer, wireless carriers have no ability or obligation to protect it from further disclosure. Customers may provide CPNI to competing carriers for analysis of more favorable rate plans, to employers for reimbursement of expenses, etc.

[9] 47 U.S.C. § 222(c)(1).

render, bill, and collect for services;[10] and to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.[11]

In its very first order after passage of the Telecommunications Act of 1996, the Commission directly addressed security concerns related to the protection of CPNI.[12] For example, the Commission ordered all telecommunications carriers to establish effective safeguards to protect against unauthorized access to CPNI by their employees or agents, or by unaffiliated third parties.[13] Further, the Commission placed the burden squarely on wireless carriers to demonstrate by clear evidence that a person has authorized the access or disclosure of CPNI pursuant to an oral or written approval.[14]

The Commission's final CPNI rules contain clear requirements for safeguarding CPNI – a rule not cited in the EPIC Petition.[15] The CPNI Safeguards rule in relevant part requires:

- carriers to train personnel as to when they are and are not authorized to use CPNI

---

[10] 47 U.S.C. § 222(d)(1).

[11] 47 U.S.C. § 222(d)(2).

[12] *In the Matter of the Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information; Use of Data Regarding Alarm Monitoring Service Providers,* CC Docket No. 96-115, Report and Order, 11 FCC Rcd 9553 (1996).

[13] *Id.* at ¶ 35.

[14] *Id.* at ¶¶ 32, 34.

[15] 47 C.F.R. § 64.2009.

- to implement an express disciplinary process for misuse of CPNI
- to maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI
- to establish a supervisory process for access to CPNI for marketing campaigns
- an officer must certify annually that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules

The rules are "flowed down" to third parties whenever disclosure of CPNI is required as part of an authorized marketing campaign or to perform some authorized service such as billing. Wireless carriers generally include strong security provisions in their agreements to require protection of CPNI maintained by these third parties and to limit use to the purpose of performance under the contract. The Commission has recognized that such controls are appropriate safeguards for CPNI, and as part of every wireless carrier's compliance obligation with the Commission's CPNI rules, such protections are built into contracts as standard operating procedure.[16]

In short, the CPNI Safeguards Rules require a compliance program for the protection of CPNI and wireless carriers have implemented these rules across the board.

B. Internal Controls – Beyond CPNI Safeguards

The CPNI Safeguards rules set a foundation for sound security practices regarding CPNI. But those rules do not stand alone in driving security practices. For

---

[16] *See In the Matter of Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* CC Docket No. 96-115 (rel. July 25, 2002) ¶ 46 ("Carriers thus remain responsible for improper use or disclosure of consumers' CPNI while in the hands of their agents").

example, all public companies must meet the requirements of the Sarbanes-Oxley Act of 2002[17] ("SOX"), which requires the adoption and implementation of policies and operational controls that address material risk. Public companies must have mechanisms in place to ensure the confidentiality, integrity and availability of information to comply.

Section 404 of SOX requires an annual certification of internal controls, an independent accountant to attest to the report and a quarterly review for necessary updates and changes.[18] In practice, because a false certification may lead to criminal penalties, detailed attention is paid to SOX requirements for security policies, IT infrastructure auditing, intrusion detection, identity management, data integrity, and vulnerability management. A discussion of the implementation of SOX in public companies obviously is not appropriate in these comments, but the Commission should take note of vast public literature available on security implementation under the law.[19] The key point is that SOX drives security planning and implementation for

---

[17] 15 U.S.C. § 7262.

[18] *See* American Institute of Certified Public Accountants' Statement on Auditing Standards (SAS) 99. According to SAS 99, weaknesses in internal controls may be present when either fraudulent financial reporting or misappropriation of assets exist. SAS 99 requires auditors to explore certain fraud activities — attitudes, rationalizations, and opportunities — to determine which threats and techniques have been most useful in perpetrating fraud. Thus, public accounting auditing includes consideration of common methods of fraud such as social engineering as well as technical weaknesses in systems that permit intrusion.

[19] For a listing of links and papers on SOX security requirements, s*ee e.g.*, http://www.knowledgeleader.com/iafreewebsite.nsf/content/Sarbanes-OxleyActCorporateGovernanceandAuditCommitteeResources?OpenDocument

all data and electronic assets maintained by a public company,[20] and that includes CPNI protection.

In concert with all of these legal requirements, wireless carriers use access controls within the company to ensure only authorized access to confidential information such as CPNI. Employment policies and agreements make clear that CPNI and other customer information is to be treated confidentially and that failure to do so may result in discipline or even termination.

Fraud threats are not limited to unauthorized disclosure of CPNI, which is why wireless carriers have security and fraud departments. The groups ensure against risk of loss of CPNI and other company assets by investigating, for example, allegations of employee or dealer fraud.[21] Before EPIC was even formed, CTIA and its members had established a solid track record in security and privacy, fighting cloning fraud, theft of electronic serial numbers (ESNs), subscription fraud and interception of communications.[22]

---

[20] While SOX applies to public companies directly, security professionals and auditors apply the SOX concepts as industry best practice to all companies.

[21] EPIC has said that they believe some carrier employees may sell CPNI. As with any company asset – from the most sensitive source code or business plan to customer personal information – employee theft will always be a risk and when discovered will always be met with swift legal action. No rule by the Commission will add any force to the existing criminal law against such theft of assets.

[22] For example, CTIA was instrumental in supporting legislative changes to criminal laws so that theft of an ESN was treated no different than theft of a credit card. *See* 18 U.S.C. § 1029(e)(1)(" the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier").

In addition to regulatory drivers for security, the Commission should not overlook contract requirements either. Wireless carriers often undertake to protect the security and confidentiality of customer information in their subscriber agreements. Just as carriers flow down security requirements to vendors and partners who receive CPNI, so too are carriers often required to implement security procedures as part of their contractual obligations, particularly in regard to customer financial information.

The Graham-Leach-Bliley ("GLB") Act requires financial institutions: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[23]

The FTC, in turn, has implemented GLB's security requirements by publishing certain "Safeguard Rules," or "standards for developing, implementing, and maintaining reasonable administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of customer information."[24]

The Safeguard Rules are very flexible and do not dictate the design of the security management program; indeed, they are notable for their simplicity. The rules require that a financial institutions develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to

---

[23] 15 U.S.C. § 6801(b).

[24] 16 C.F.R. § 314.1(a).

the entity's size and complexity, the nature and scope of activities, and the sensitivity of any customer information at issue.[25]

Financial institutions "flow down" security requirements to their financial services vendors. Wireless carriers often negotiate security requirements with financial institutions when services fall within the requirements of the law. GLB is a useful analogy for the Commission in considering security issues, but the key point here is that GLB often turns out to be a driver in carrier security planning and negotiations.

In addition, and as a further result of GLB, wireless carriers that accept credit cards for payment for services are being required by the card associations such as Mastercard and Visa to meet the Payment Card Industry Data Security Standard. The Standard's requirements for network and systems monitoring, auditing, access control measures, and a vulnerability control program apply to all merchants that store, process or transmit cardholder data.[26]

Accordingly, there are and will continue to be significant regulatory and contractual incentives for wireless carriers to adopt and maintain strong security. New rules directed at CPNI alone would offer no additional protection but would increase compliance costs for wireless carriers and potentially diminish customer access to their own CPNI as discussed below.

---

[25] 16 C.F.R. § 314.3.

[26] The PCI Data Security Requirements can be found at http://66.102.7.104/search?q=cache:caGbxvYs0acJ:usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf+PCI+Data+Security+Standards&hl=en

C. Wireless Carrier Promises to Customers

The leading wireless carriers also subscribe to CTIA's Consumer Code for Wireless Service, which requires the participating carrier to adopt and publish a privacy policy that explains its information practices to customers.[27] We think it is useful for the Commission to examine those publicly available and posted privacy policies to see the commitments wireless carriers have made to their customers in regard to security of personal information. For example, Cingular Wireless states as follows:

> **Network and Information Security**
>
> We maintain a variety of physical, electronic, and procedural safeguards to guard your personal information. For example, we use accepted tools and techniques to protect against unauthorized access to our systems. Also, we grant access to personal information about you to employees and contractors who need to know that information to provide products or services to you. In addition, we work to protect the security of your personal information when you are ordering new service via the Cingular Wireless Web site by using well-known Internet encryption technologies like Secure Sockets Layer (SSL). We also use encryption technologies to protect your account information when you are viewing your bill on our Web site. You should be aware that Cingular Wireless has no control over the security of other sites on the Internet you might visit, interact with, or from which you buy products or services.
>
> **What Can I Do to Protect My Personal Information?**
>
> An important part of ensuring the security of personal information is your own effort to protect against unauthorized access to your wireless device and the personal information contained in it and on your SIM card. Most phones and wireless PDA-type devices store calling information both in the phone

---

[27] *See* http://www.ctia.org/wireless_consumers/consumer_code/index.cfm

> and on the SIM card. Therefore, before discarding your phone or PDA, trading it in or giving it away, be sure you remove and retain your SIM card and follow the manufacturer's instructions for deleting all personal information on the device itself. (This can be found in your owner's manual or on the manufacturers' Web site).
>
> In addition, use passwords to prevent unauthorized access to your wireless device, your wireless service account, and your voicemail. If you write down your passwords or user names, keep the information in a secure location. Do not give your password to someone else unless you intend them to have the same full access and ability to make changes to your account as you have. Change your passwords periodically.[28]

Some carriers also have a Code of Business Conduct that addresses privacy and security. The Verizon Wireless Code states:

> We provide services that reach deep into the personal and business lives of our customers. Our customers trust us with their account information, records and communications data. Maintaining our customers' privacy is a responsibility that we take seriously. Verizon Wireless has an FCC regulatory duty to protect the confidentiality of Customer Proprietary Network Information (CPNI). CPNI is defined as information that relates to the quantity, technical configuration, type, destination, and amount of use of our service subscribed to by our customers and that is made available to us by our customers by virtue of our relationship and information contained in bills pertaining to service we provide and services for which we bill. You may only use CPNI we receive about our customers for certain approved Verizon Wireless business purposes. We may also disclose CPNI upon written request by the customer or in response to legal

---

[28] *See* http://www.cingular.com/privacy/privacy_policy#11; *see also* Verizon Wireless Privacy Statement at http://www.verizonwireless.com/b2c/footer/privacy.jsp ("We require our employees to protect the privacy of information about our customers and expect our partners and suppliers to do so as well. You can feel confident that your individual information will be protected when you access your account or order products or services from our websites.")

> process. Depending upon the nature of the CPNI there are clear "opt-in" (affirmative, express consent after appropriate notification in compliance with the law) and "opt-out" (consent is deemed to have been given after appropriate notification in compliance with the law) approval requirements. We have clear policies and procedures regarding compliance with legal requirements and the use of CPNI. Please contact your supervisor or the Legal Department if you have any questions about the use of CPNI.[29]

As the Commission knows, privacy and security representations to customers must not be made lightly. The FTC has taken a firm stand on privacy and security representations, rigorously enforcing consumer protection law against unfair or deceptive trade practices.[30] The FTC enforcement cases make clear that it vigorously enforces its privacy rules.[31]

D. Customer Service Protections

Customer service is important to wireless carriers and their customers. In 2004, JD Powers reported that more than half of cellular phone users had contacted the customer-service department for assistance within the last year.[32] Among those who contact their carriers, Powers reported 71 percent do so via telephone and 26

---

[29] Verizon Wireless Code of Business Conduct *available at* http://cache.vzw.com/pdfs/aboutus/Verizon_Book_Internet.pdf.

[30] 15 U.S.C. § 45(a) prohibits unfair or deceptive trade practices.

[31] *See e.g., In re BJ's Wholesale Club, Inc.*, No. C-042 3160 (settled May 17, 2005)(FTC enforcement action for failure to protect security of customer information), *available at* http://www.ftc.gov/os/caselist/0423160/0423160.htm

[32] http://www.jdpower.com/cc/global/pr/search.asp

percent through the carriers' retail stores. E-mail/Internet contacts account for only 3 percent.[33]

Based on these statistics, the Commission should understand that wireless carriers respond to millions of customer service calls each year. Surely, the Commission does not want to adopt rules that would impede wireless customers' access to their own account information.[34] Rules that require in-person customer service would be a giant step backwards from the convenient and responsive customer service wireless carriers provide over the telephone and Internet.

Instead, it is fair and balanced to rely on customer service representatives who are trained to identify fraudulent attempts to gain access to customer information. These representatives are well-trained and employ multi-factor authentication to ensure the requesting party is authorized to receive the information. For example, customer service representatives certainly are well aware of the need to verify identity whenever an address change for billing is requested.

E. Customer Notification of Security Breaches and Identity Theft Protections

In July 2003, California Senate Bill 1386 went into effect, becoming the first law in the Nation to establish notification requirements regarding security breaches that involve the compromise of personal information. Since that time, 20 more states

---

[33] *Id.*

[34] The harms EPIC asks the Commission to address would not be prevented even by requiring wireless customers to appear in person at their carrier's premises. A determined thief that has access from other sources to sufficient information to create a false identity before reaching the wireless carrier will be able to appear as the customer. Identity theft is what permits the criminal to gain access to CPNI in the first place.

have passed similar legislation,[35] and Congress is considering enacting a uniform federal security breach notification statute.[36] While none of these laws require notification upon the disclosure of calling records alone, notification of affected consumers generally is required for unauthorized disclosure of personal information coupled with an account number and access code or other nonpublic information such as a social security number or driver's license number.[37]

As a general matter, wireless carriers report very few complaints about disclosure of CPNI to incorrect or unauthorized recipients, especially given the account access they provide to nearly 200 million wireless subscribers. This no doubt comports with the Commission's own experience. As far as CTIA can determine, the Commission has reported no such customer complaints in its quarterly report of consumer inquiries and complaints.[38] Any wireless carrier that receives such a complaint would investigate it thoroughly and take appropriate action.

---

[35] For a chart of the notification laws of each State, the effective dates thereof and a summary of the requirements, *see* http://www.perkinscoie.com/content/ren/updates/privacy/092605.htm

[36] *See* Identity Theft Protection Act, S. 1408; Comprehensive Identity Theft Prevention Act, S. 768; Personal Data Privacy and Security Act of 2005, S. 1332; Notification of Risk to Personal Data Act, S. 1326.

[37] While these laws help alert consumers to the risk of identity theft, it is difficult to imagine what benefit consumers would derive from a notice of disclosure of phone records as EPIC requests. Phone records may reveal personal information about who a customer calls but they do not provide a predicate for identity theft.

[38] *See e.g.*, Quarterly Report On Informal Consumer Inquiries And Complaints Released (Sept. 28, 2005) available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-261287A1.doc (no complaints from consumers regarding unauthorized disclosure of CPNI).

And customers have strong protection under the Fair and Accurate Credit Transactions Act ("FACT Act")[39] should they become a victim of identity theft. Before a carrier can extend credit to a customer who has placed a fraud alert with a credit bureau, the carrier must take reasonable steps to identify the putative customer.[40] The FACT Act also grants significant consumer rights in fighting identity theft, including the requirement that entities provide individuals with records related to acts of identity theft, which, in the case of wireless carriers, would include subscription information and CPNI generated on a fraudulent account.[41]

Identity theft, of course, continues to be a major enforcement priority for state and federal authorities. Most states have laws that criminalize identity theft.[42] State

---

[39] 15 U.S.C. §§ 1681 *et seq.*

[40] *Id.* Section 112 of the FACT Act states that no user of a consumer report is permitted to extend credit to a consumer whose credit report contains an alert "unless the user [of the report] utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request." The Commission should note that even in those cases where a prior fraud is known to have occurred, neither Congress nor the FTC in implementing the law have dictated specific "know your customer" procedures.

[41] *See* 15 U.S.C. 1681g ("a business entity that has provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim, shall provide a copy of application and business transaction records in the control of the business entity" to the victim or as directed by the victim to the police.)

[42] For a list of state identity theft statutes, *see* http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm

attorneys general are on the front lines of enforcing these statutes and are more than capable of doing so.[43]

Just like other businesses that must access their customers' personal information and make it available for customer service or other reasons, wireless carriers are not immune from schemes to defraud them or their customers. When unauthorized intrusions take place, wireless carriers cooperate with law enforcement to identify the criminal and vigorously support prosecution and sentencing efforts. For example, in the much publicized disclosure of Paris Hilton's address book on the Internet, the identification of the criminal and his prosecution would not have been possible without the assistance of the wireless carrier.[44] In that case, the teenage hacker, who also compromised the systems of Lexis-Nexus, was sentenced to 11 months in prison.[45]

Wireless carriers likewise have taken aggressive steps to combat "social engineering" and other fraudulent schemes to access customer information. Verizon Wireless recently filed suit against an information broker who obtained calling records from Verizon Wireless's customer service representatives by deceptive and

---

[43] The states have an important responsibility in consumer protection. For decades, state Attorneys General have safeguarded citizens by their vigorous enforcement of state unfair trade practice and consumer protection laws. CTIA recognizes the states' traditional consumer protection role and supports their authority to enforce these laws of general applicability. *See In the Matter of Truth-in-Billing and Billing Format*, CC Dkt. 98-170, CTIA Reply Comments at 35 (July 25, 2005). http://files.ctia.org/pdf/filings/050725_TIB_Reply_Comments.pdf

[44] In that case, the customer obviously knew about the access to personal information and a notice rule would have been meaningless.

[45] *See* http://www.eweek.com/article2/0,1895,1859128,00.asp

fraudulent means.[46] On September 13, 2005, Verizon obtained a permanent injunction against the defendants and their agents or partners from "directly or indirectly acquiring, possessing and/or selling information regarding Verizon Wireless's customers without valid judicial process or the customers' express written consent.[47]

F. EPIC'S Additional Security Elements

To the extent that the foregoing discussion has not directly addressed the security issues raised by EPIC, CTIA now addresses several specific points in the EPIC Petition. EPIC contends that unique passwords for any access to account information would greatly increase security. But that is naïve. In fact, customers often use a single passcode for multiple accounts, which if compromised or shared for another purpose can be provided to (or devined by) the information broker, and customers frequently forget passcodes, write them down where the code can easily be found by others or misplace that paper. They then call customer service to obtain the passcode and the cycle is repeated.

For those carriers that offer online access to customer accounts as a customer service, a personal password selected by the customer generally is the required access key. Unauthorized access of a consumer account is a felony.[48] Even in these cases, carriers receive a large number of requests for password assistance. In providing the password, carriers use an extra degree of caution, usually providing it only to the email address of the subscriber.

---

[46] *Verizon Wireless v. Source Resources,* Complaint, Somerset County Sup. Ct., NJ, filed July 8, 2005.

[47] *See id.,* Permanent Injunction on Consent (Sept. 13. 2005).

[48] 18 U.S.C. § 1030.

EPIC further calls for audit trails regarding access to CPNI. Again, without discussing the details of carrier security procedures, the Commission can be assured that indeed, such procedures exist. The Commission's Safeguard Rules require it. Customer service notes, access controls, log access files and other documentation exists and is maintained. Again, auditing is no panacea for fraud prevention. An audit trail that provides a record of a disclosure is only of use when someone complains about or reports a violation. As noted above, CTIA is not aware of any such complaints in the industry despite EPIC's identification of dozens of putative online call record brokers.

EPIC also calls for encryption of calling records in storage. If the threat of disclosure of calling records truly was from brute force or other hacking attack on carrier databases, then the suggestion might be worthy of debate. But the evil EPIC seeks to prevent is the disclosure of call records to persons claiming to be the customer. Obviously, such records would have to be accessed and disclosed in unencrypted form to the customer. Imposing such an encryption requirement on carriers would increase their expense, slow down customer service access to records in response to the many legitimate inquiries received from customers, and vastly complicate carrier storage and access methods with no corresponding benefits.

EPIC also calls for deletion of calling records when they are no longer needed for billing or dispute purposes. Alternatively, EPIC calls for removal of personally identifying information from the records after some period of time. 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. No law requires such data destruction, and no security principle makes older records more

susceptible or newer records less susceptible to fraudulent disclosure. In short, the remedy has no relationship to the problem cited by EPIC.

The EPIC Petition reveals legitimate concern for customer privacy. CTIA and its members share that concern. But EPIC is no security professional. And its recommendations reflect a lack of understanding of security fundamentals.

II. CONCLUSION

CTIA and its members share EPIC's concerns for the confidentiality of CPNI, but we strongly disagree with any suggestion that carriers are lax in their duty to protect it. CTIA and its members do not take security lightly, nor do they disregard the confidentiality of CPNI for convenience. Instead, wireless carriers take security seriously, comply with the law, and protect the privacy of their customers.

To be sure, no system is foolproof, especially one that handles millions of customer service calls each year without the customer being present. But existing security practices and law are sufficient to ensure carrier vigilance against such fraud. As for information brokers and data thieves, CTIA supports the strongest measures against those who traffic in personal information in unlawful or deceptive ways. Congress is considering laws to regulate information brokers today; and the FTC has particular expertise in enforcing the law against those who deceptively advertise the ability to obtain calling records under the pretence that doing so is somehow legal without the consent of subscriber. As FTC Chairwoman Majoras told Congress recently:

> One particular focus of concern [of the FTC] has been "data brokers," companies that specialize in the collection and distribution of consumer data. Data brokers epitomize the

tension between the benefits of information flow and the risks of identity theft and other harms.[49]

For all of these reasons, the EPIC Petition should be denied, and instead, the Commission should cooperate with the FTC should it choose to investigate the illicit activities of information brokers who purport to sell call records.

Respectfully submitted,

/s/ Michael Altschul

Michael F. Altschul
Senior Vice President, General Counsel

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

October 31, 2005

Its Attorneys

[49] *See* Prepared Statement of the Federal Trade Commission on Data Breaches and Identity Theft, Presented by Chairman Majoras and the Other Members of the Commission Before the Committee on Commerce, Science, and Transportation of the United States Senate **(**June 16, 2005), *available at* http://www.ftc.gov/opa/2005/06/datasectest.htm