

**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)	RM-11277
For Access to Customer Proprietary)	
Network Information)	

REPLY COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

CTIA – The Wireless Association® (“CTIA”)¹ submits these reply comments in response to the reply comments filed by the Electronic Privacy Information Center (“EPIC”) concerning enhanced security and authentication standards for access to Customer Proprietary Network Information (“CPNI”).² For the reasons set forth in this reply and CTIA’s Comments in Opposition to EPIC Petition for Rulemaking, the Commission should deny the EPIC Petition for Rulemaking.³ Instead, CTIA urges the Commission to work with the Federal Trade Commission (“FTC”) to prosecute the

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 Reply Comments of the Electronic Privacy Information Center, CC Dkt. 96-115, RM-11277 (Nov. 9, 2005) (“EPIC Reply Comments”).

³ CTIA-The Wireless Association® Comments in Opposition to EPIC Petition for Rulemaking, CC Dkt. 96-115, RM-11277 (Oct.31, 2005) (“CTIA Opposition”); Electronic Privacy Information Center Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Dkt. No. 96-115, RM-11277 (Aug. 30, 2005) (“EPIC Petition”).

information brokers who unlawfully victimize carriers and their customers by obtaining and selling customer information.

I. ADDITIONAL RULES ARE UNNECESSARY

The parties submitting comments on the EPIC Petition have demonstrated their commitment to safeguarding customers' information.⁴ Carriers, in full compliance with CPNI and state privacy laws, have instituted appropriate procedures to protect customer confidentiality while still providing customers with access to their own account information. Confusing the victim with the information brokers who steal customers' identities to obtain account information (through "pretexting"), EPIC argues carriers' practices are responsible for security problems and urges the FCC to initiate a rulemaking to enhance safety measures and authentication standards for CPNI.⁵ CTIA believes new rules are not the answer, as the imposition of redundant and inflexible security rules would not curtail the fraudulent activity, but would impose considerable costs on carriers and ultimately consumers.⁶

The EPIC Reply Comments acknowledge that no single security system is ideal and that no single method can produce a secure system.⁷ CTIA agrees with EPIC that carriers must be allowed the flexibility to adopt different approaches to secure customer

⁴ See Comments of Verizon Wireless, RM-11277 at 2 (Oct. 31, 2005) ("Verizon Wireless Comments"); Opposition of BellSouth Corporation, RM-11277 at 3 (Oct. 31, 2005) ("BellSouth Opposition"); Comments of Verizon, RM-11277 at 2 (Oct. 31, 2005) ("Verizon Comments"); Comments of SBC Communications Inc., CC Dkt. No. 96-115, RM-11277 at 1 (Oct. 31, 2005) ("SBC Comments").

⁵ See EPIC Reply Comments at 1.

⁶ See SBC Comments at 3.

⁷ See EPIC Reply Comments at 3.

account information and combat the theft of this data.⁸ Consequently, the EPIC request for a rulemaking to develop and establish a security standard that heightens the privacy of CPNI is not the optimal solution. Continued vigilance and carrier-specific security tactics coupled with coordinated efforts among the FCC, FTC, and carriers is the best means to thwart wrongdoers from unlawfully obtaining confidential customer communications and records.

EPIC mistakenly asserts that CTIA urges the FCC to “defer” to the FTC and requests that the FCC allow the FTC to enforce its laws against online data brokers.⁹ Rather, CTIA recommends both agencies work together to bring the online data brokers and private investigators, the true offenders, to justice.¹⁰ CTIA supports comments suggesting that a joint task force be formed that will assist the industry to track and combat persons who unlawfully obtain and sell customer information.¹¹ The EPIC Petition proposes a number of security measures carriers may implement to more adequately protect access to CPNI.¹² The joint task force could also evaluate EPIC’s recommendations as well as other innovative measures, such as a hotline or website link to report suspected illegal activity.¹³

EPIC also renews its request for an investigation of carrier practices, but in the face of unanimous criticism that this actually would harm security by providing a roadmap to guide information brokers around the barriers carriers’ have erected to protect

⁸ See EPIC Reply Comments at 4.

⁹ See *id.* at 7.

¹⁰ See CTIA Opposition at 2, 21.

¹¹ See Verizon Wireless Comments at 5; Verizon Comments at 5.

¹² See EPIC Petition at 11-12.

¹³ See Verizon Comments at 5.

customer account information.¹⁴ EPIC states that carrier specific security procedures need not be published in the record.¹⁵ CTIA believes that no purpose would be served in the FCC collecting this information on or off the record. The FCC, despite its best intentions, cannot be expected to be an expert in the rapidly evolving and technically complex area of data security and the complexity and variety of carriers' systems.

As CTIA stated in its comments, the Commission should deny the EPIC Petition to implement mandated security rules for the following reasons: (1) additional rules would be both duplicative and under-inclusive, yielding no consumer benefit; (2) in a matter of time, wrongdoers will circumvent mandated measures, which will likely become obsolete and ineffective in the long-term; and (3) carriers' expenses would increase, wherein consumers would ultimately have to bear these costs.¹⁶ As an alternative, the FCC, FTC and carriers should vigorously enforce existing laws and hold information brokers accountable for their acquisition and sale of illegally and fraudulently obtained customer records. CTIA agrees with Verizon that an "offensive strike at wrongdoers will be far more effective at eliminating the problem than any defensive measures that carriers or the Commission can adopt."¹⁷

¹⁴ See CTIA Opposition at 3; Verizon Wireless Comments at 5; Verizon Comments at 1.

¹⁵ See EPIC Reply Comments at 5.

¹⁶ See CTIA Opposition at ii; SBC Comments at 2; Verizon Comments at 3.

¹⁷ Verizon Comments at 6.

CONCLUSION

For the foregoing reasons, CTIA respectfully requests that the Commission deny the EPIC Petition. CTIA urges the Commission to cooperate with the FTC to prosecute information brokers who use unlawful methods to obtain confidential customer information.

Respectfully submitted,

CTIA - THE WIRELESS ASSOCIATION®

/s/ Marlo Go _____

Michael F. Altschul
Senior Vice President & General Counsel

Marlo Go
Staff Counsel

Its Attorneys

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

November 15, 2005

CERTIFICATE OF SERVICE

I, Marlea Leary, hereby certify that, on this 15th day of November, 2005, a copy of the foregoing “Reply Comments of CTIA-The Wireless Association®” in RM-11277 was served on counsel for Petitioners, Chris Jay Hoofnagle, Senior Counsel, EPIC West Coast Office, 944 Market Street, Suite 709, San Francisco, CA 94102, by expedited mail, and by electronic mail to hoofnagle@epic.org.

/s/ Marlea Leary _____