

**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;)	
)	
IP-Enabled Services)	WC Docket No. 04-36
)	

REPLY COMMENTS OF T-MOBILE USA, INC.

William F. Maher, Jr.
Joan E. Neal
MORRISON & FOERSTER LLP
2000 Pennsylvania Ave., N.W.
Washington, D.C. 20006-1888
202.887.1500

Attorneys for T-Mobile USA, Inc.

Thomas J. Sugrue
Vice President Government Affairs
Kathleen O'Brien Ham
Managing Director, Federal Regulatory
Affairs
Sara F. Leibman
Director, Federal Regulatory Affairs
Shellie Blakeney
Corporate Counsel, Federal Regulatory
Affairs
T-Mobile USA, Inc.
401 9th Street, N.W.
Suite 550
Washington, D.C. 20004

August 7, 2007

TABLE OF CONTENTS

	Page
I. SUMMARY AND INTRODUCTION	1
II. THE RECORD DOES NOT SUPPORT FURTHER EXPANSION OF THE CPNI RULES AT THIS TIME	2
A. The FCC Should Not Expand the Call-In Password Requirement to Non- Call Detail CPNI	2
B. The Record Does Not Support Adoption of an Audit Trail Requirement	4
C. The FCC Should Not Adopt Mandatory Encryption Requirements for CPNI.....	5
D. The Record Does Not Support Commission Action Limiting Data Retention	6
E. The FCC Should Not Adopt New Rules at this Time Regarding the Protection of Information Stored in Mobile Communications Devices.....	7
F. The Commission Should Not Adopt the EPIC Coalition’s Additional Proposals	9
III. CONCLUSION	10

**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;)	
)	
IP-Enabled Services)	WC Docket No. 04-36
_____)	

REPLY COMMENTS OF T-MOBILE USA, INC.

I. SUMMARY AND INTRODUCTION.

In response to comments on the above-captioned further notice of proposed rulemaking (“FNPRM”), T-Mobile USA, Inc. (“T-Mobile”)¹ urges the Commission to refrain from imposing additional regulations governing customer proprietary network information (“CPNI”) at this time. The overwhelming majority of commenters agree with T-Mobile that carriers already take seriously the protection of their customers’ privacy, and that the Commission should evaluate the impact of the regulations and laws now in place to protect CPNI before promulgating additional rules. As T-Mobile explained in its initial comments, the combined protections afforded by the extensive CPNI rules recently adopted by the Commission² and the passage of the Telephone

¹ T-Mobile is one of the major national wireless carriers in the United States, with licenses covering 46 of the top 50 U.S. markets and serving over 25 million customers with a network reaching over 275 million people (including roaming and other agreements).

² *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Report &

Records and Privacy Protection Act (“TRPPA”), which criminalized pretexting, should be allowed to operate before the Commission takes further action. The EPIC Coalition and the New Jersey Division of Rate Counsel (“NJDRRC”), the only two commenters that request additional regulation in this area, do not demonstrate that such regulation is necessary.³

II. THE RECORD DOES NOT SUPPORT FURTHER EXPANSION OF THE CPNI RULES AT THIS TIME.

A. The FCC Should Not Expand the Call-In Password Requirement to Non-Call Detail CPNI.

Based on the initial comments, the Commission should refrain from expanding the password requirement in situations when customers call carriers for assistance concerning non-call detail CPNI. Such an expanded requirement would significantly inconvenience customers who want to resolve routine billing questions and problems without delay or disruption, and would do little to enhance consumer privacy.⁴

The EPIC Coalition seeks an across-the-board imposition of mandatory passwords.⁵ T-Mobile, however, has extensive real-life experience that reflects customers’ negative reactions to mandatory passwords and demonstrates that customers highly value convenience when calling its Customer Care department. As T-Mobile has stated in this proceeding, at one point it required its customers to use passwords for call-in access on all accounts. Based on customer

Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (“*New CPNI Order*” or “FNPRM,” as appropriate). All comments and reply comments cited herein refer to comments filed in this proceeding on July 9, 2007, unless otherwise stated.

³ See Comments of Consumer Action, et al. (“EPIC Coalition”) at 6-26; see New Jersey Division of Rate Counsel (“NJDRRC”) Comments at 4-7.

⁴ See AT&T Comments at 5; Sprint Nextel Comments at 6-10; Verizon Comments at 3-8.

⁵ See EPIC Coalition Comments at 6-7.

feedback, however, T-Mobile changed to optional passwords for call-in access.⁶ T-Mobile has dedicated itself to providing responsive customer service as one way to differentiate its services from those of other wireless carriers and regularly receives awards recognizing its efforts in this regard.⁷ T-Mobile should not be required to reestablish a practice that caused such a high level of customer dissatisfaction.

The Commission should preserve flexibility for carriers to maintain customer-friendly practices. Contrary to the claims of the EPIC Coalition and NJDRC, an expanded password requirement for call-in access will neither reduce consumer confusion nor increase consumer satisfaction.⁸ The record in this proceeding⁹ and T-Mobile's own experience demonstrate that mandatory passwords are burdensome to consumers and disrupt their ability to resolve billing and other issues promptly and efficiently. A critical component of T-Mobile's exceptional customer service is its ability to fashion flexible policies that work well for customers while also protecting their privacy. In this regard, the EPIC Coalition and NJDRP fail to demonstrate that

⁶ See T-Mobile 2006 Comments at 11 (Apr. 28, 2006).

⁷ T-Mobile has received awards six consecutive times from J.D. Power and Associates for (i) providing the highest level of customer service in the wireless industry, and (ii) overall customer satisfaction among wireless telephone users in all regions surveyed. See J.D. Power and Associates Press Release, *J.D. Power and Associates Reports: Wireless Carriers Show Steady Improvement in Timeliness of Resolving Customer Care Issues: T-Mobile Ranks Highest in Wireless Customer Care Performance for a Sixth Consecutive Reporting Period* (July 25, 2007) available at <http://www.jdpower.com>; Jeffrey Bartash, *Wireless Customers Found More Satisfied; T-Mobile Again In Lead, J.S. Power Says; AT&T Improves; Sprint Lags*, MarketWatch (July 25, 2007) ("For the sixth straight time, T-Mobile finished at the top of the consumer-satisfaction survey, scoring 108 points.").

⁸ See EPIC Coalition Comments at 7; see NJDRC Comments at 6-7.

⁹ See, e.g., *New CPNI Order*, 22 FCC Rcd at 6936 n.47 ("We understand that many consumers may not like passwords..."); Sprint Nextel Comments at 6-10; Verizon Comments at 3-9; AT&T Comments at 5 (noting that requirements like the mandatory passwords impose significant burdens on customers without any commensurate benefits, and citing studies that demonstrate customers oppose mandatory passwords).

pretexters are even interested in the type of information that would be protected by the expansion of mandatory passwords. The Commission should not expand the call-in password requirement.

B. The Record Does Not Support Adoption of an Audit Trail Requirement.

The record continues to demonstrate that the cost of requiring audit trails far outweighs any consumer benefits.¹⁰ Neither the EPIC Coalition nor the NJDRC offer any new evidence to justify such regulations. As T-Mobile explained in its 2006 and 2007 comments,¹¹ the Commission found credible evidence as far back as 1999 that the implementation of an audit trail requirement could cost tens of millions of dollars per carrier.¹² The requirement was eliminated after the Commission concluded that, in light of preexisting rules requiring protection of CPNI, mandating audit trails would be duplicative and costly, without corresponding consumer benefits.¹³ Nothing in the record indicates the Commission should depart from this pro-consumer decision.

Mandating adoption of audit trails also could be counterproductive in law enforcement efforts to investigate and punish pretexters. The EPIC Coalition, claiming that audit trails could help law enforcement detect pretexting activities, ignores evidence that regulations that

¹⁰ See Sprint Nextel Comments at 11-12 (noting that the costs involved in implementing audit trails across different systems are considerable, and could substantially outweigh any consumer benefits); see Time Warner, Inc. Comments at 9 (arguing that “requiring carriers to record all instances when a customer’s records have been accessed, whether information has been disclosed, and to whom, would be extremely burdensome and of limited value in fighting pretexting.”)(citation omitted); see NuVox Communications and XO Communications Joint Comments at 5-6.

¹¹ See T-Mobile 2006 Comments at 16; see T-Mobile Comments at 4-5.

¹² See *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14474-14475 (1999).

¹³ *Id.* at 14475.

micromanage or provide a “road map” of audit trails could in fact hinder efforts to catch pretexters.¹⁴ Because carriers already monitor customer interactions in a variety of ways, “disrupting established processes and systems with a new set of regulatory requirements ... may inadvertently hinder carriers’ efforts to assist law enforcement agencies in investigating pretexters.”¹⁵

C. The FCC Should Not Adopt Mandatory Encryption Requirements for CPNI.

The EPIC Coalition failed to provide a reasoned basis for its proposal to require encryption of all stored CPNI.¹⁶ Contrary to the EPIC Coalition’s comments, a Commission rule mandating data encryption is not necessary to protect the confidentiality of customer data from unauthorized employees inside the carrier. T-Mobile, for example, already has in place an express disciplinary process to address noncompliance with company policies, including policies regarding employee use of, access to, and disclosure of CPNI.¹⁷ Carriers should have the flexibility to implement processes that are most compatible with their business operations, and new requirements could remove this flexibility.

¹⁴ EPIC Coalition Comments at 8-9.

¹⁵ See T-Mobile Comments at 5. See also Sprint Comments at 11 (audit trails are of limited use to law enforcement investigations, because at best they confirm that the pretexter gave correct answers to the authentication questions); Verizon Comments at 14 (an audit trail is not helpful in preventing account access by data brokers and pretexters since the audit trail may only reveal that someone purporting to be the customer called and asked about account details).

¹⁶ See EPIC Coalition Comments at 10.

¹⁷ T-Mobile 2006 Comments at 9 (“T-Mobile has implemented numerous safeguards, policies and procedures to protect customer records from unauthorized disclosure...T-Mobile requires thorough training of customer-facing personnel who must access customer records in order to respond to customer inquiries...employees also are required to sign confidentiality agreements that specifically cover the handling of customer information...[e]mployees face disciplinary action, up to and including termination, for failure to follow T-Mobile’s confidentiality policies and procedures...T-Mobile conducts internal investigations and audits that evaluate the security of customer data.”).

New encryption requirements are similarly unnecessary to prevent unauthorized access to CPNI during the physical transfer of CPNI among carrier affiliates, independent contractors, and joint venture partners. As T-Mobile has explained previously, there is no evidence cited in the FNPRM or in the record that data brokers have successfully circumvented carriers' current protection measures during such a physical transfer.¹⁸ New encryption requirements would impose significant costs on carriers and their customers. Further, rules that specifically describe a method of protecting CPNI while in transit effectively provide a roadmap for data brokers and hackers on how to compromise carriers' systems. Rather than require particular data protection methods, T-Mobile urges the Commission to allow carriers the discretion to craft CPNI protection mechanisms suited to their current systems and customers' needs.

D. The Record Does Not Support Commission Action Limiting Data Retention.

Limiting data retention by carriers could hinder law enforcement efforts, could conflict with other FCC and state law requirements governing record retention, and may run afoul of obligations adopted by carriers in national security agreements.¹⁹ The EPIC Coalition's claim that limitations on data retention enhances CPNI protection is unsupported, particularly in light of the lack of evidence suggesting that data brokers are interested in older information.²⁰ The Coalition's recommendation that the Commission require de-identification of call records that carriers retain for certain purposes is likewise not useful in light of all the safeguards already adopted by carriers to protect their customers' privacy.

¹⁸ T-Mobile Comments at 6.

¹⁹ See AT&T Comments at 8; Comcast Comments at 9-10; Verizon Comments at 17-20.

²⁰ EPIC Coalition Comments at 13-14.

The EPIC Coalition’s call for a rule banning the sale of aggregated CPNI data is similarly unnecessary and appears to be outside the scope of the FNPRM and contrary to the Communications Act.²¹ Section 222 of the Communications Act specifically permits “[a] telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service [to] use, disclose, or permit access to aggregate customer information.”²² This particular CPNI provision has not been at issue in this proceeding, and the record contains no indication that it has caused any harm to customers. There is no legal or policy basis for the Commission to issue rules prohibiting what the Act clearly allows.

E. The FCC Should Not Adopt New Rules at this Time Regarding the Protection of Information Stored in Mobile Communications Devices.

T-Mobile's public website already provides instructions and guidance to customers on how to delete or erase personal data from their handsets prior to discarding or refurbishing such equipment. Through this approach, customers maintain control over the information that they may enter into their handsets.²³

The EPIC Coalition now seeks multiple, redundant regulations to address the risk of consumer data privacy breaches involving mobile handsets. Their proposals include requiring carriers to erase mobile devices under various circumstances, enabling remote deletion for lost

²¹ See *id.* at 13-14.

²² See 47 U.S.C. § 222(c)(3), (h)(3).

²³ See AT&T Comments at 9 (“[D]ecisions about what personal data to store, or not to store, on a mobile device rest with the consumer. Carriers do not typically have access to such information and play no role in determining what information a consumer chooses to store on mobile devices or how that information is used.”); see Sprint Nextel Comments at 20 (“Wireless carriers are not well-positioned to guarantee the privacy of customer information stored on devices that suppliers manufacture and which are in the physical control and custody of customers.”).

and stolen devices, mandating that manufacturers implement hardware or firmware based solutions for data deletion, including storing personal information on removable flash memory cards, and carriers or manufacturers redesigning mobile device software user interfaces to make deletion a more easy-to-find feature.²⁴ Each of these regulations is broad in scope and could require the retrofitting or redesign of the mobile device. Implementing all of these regulations simultaneously, as the EPIC Coalition appears to advocate, is completely unnecessary and without demonstrable benefit to consumers.

Though the EPIC Coalition concedes that “the costs of implementing the above suggestions might be substantial...,”²⁵ it fails to show that benefits to the consumer from these proposals exceed the cost to the industry, and ultimately consumers, of complying with these myriad proposed regulations.²⁶ Not only would these multiple measures impose substantial cost and implementation burdens on consumers, manufacturers, and carriers alike, the EPIC Coalition apparently is seeking regulation of data not within Section 222’s definition of CPNI. The Trust Digital study focuses on the fact that consumers may choose to store personal and corporate information including company records, product information, address books, calendar entries, and medical information on their wireless mobile devices.²⁷ The Commission’s authority to

²⁴ See EPIC Coalition Comments at 14-20.

²⁵ See *id.* at 18.

²⁶ See *id.* at 15-16. The EPIC Coalition's sole piece of evidence of the actual harm resulting from the passage of personal information stored on mobile devices to unauthorized parties was a press release issued by Trust Digital, a for-profit company that markets “enterprise smartphone security and management software.” See Trust Digital Home Page, at <http://www.trustedigital.com> (last visited July 31, 2007).

²⁷ Trust Digital Press Release, *Used Smartphones and PDAs for Sale on eBay Reveal Massive Volume of Sensitive Data* (Aug. 30, 2006).

promulgate regulations to protect non-CPNI is uncertain, especially when such data, entered by consumers for their own use, is outside the definition of CPNI in Section 222.²⁸

T-Mobile has a formal process in place for removing information stored on handsets that are resubmitted to T-Mobile for purposes of recycling and for handsets that are refurbished. Handsets are “flushed” and essentially restored to their factory default settings. In addition, T-Mobile has instructions for customers on its website for removing stored information on handsets in the event they give their handsets to a third party (other than T-Mobile).²⁹

Further, Commission regulation is unnecessary and inappropriate to safeguard the integrity of personal or corporate information stored on mobile devices. Industry-lead hardware and software designs and consumer-initiated data protection strategies will be better tailored to individual customer needs and more in tune with the pace of technological advances than any one-size-fits-all regulation the FCC could implement.

F. The Commission Should Not Adopt the EPIC Coalition’s Additional Proposals.

The Commission also should not adopt the broad opt-in regime the EPIC Coalition proposes.³⁰ This sweeping requirement apparently would require customer notification and opt-

²⁸ See 47 U.S.C. § 222 (h)(1).

²⁹ See T-Mobile Comments at 8 n25. See T-Mobile.com, *How Can I Delete Data from My Device?*, <http://support.t-mobile.com/knowledgebase/root/public/tm20506.htm#all> (last visited Aug. 6, 2007) (setting forth instructions on how to delete data from mobile devices); T-Mobile.com, *Safety, Community & Sponsorships*, http://www.t-mobile.com/Company/Community.aspx?tp=Abt_Tab_HandsetRecycling (last visited Aug. 6, 2007) (advising customers to ensure that they have deleted data from their handsets prior to participating in handset recycling program); and T-Mobile.com, *What should I do with my old Subscriber Identity Module (SIM) card(s)?*, <http://support.t-mobile.com/knowledgebase/root/public/tm23344.htm> (last visited Aug. 6, 2007) (explaining how to delete data on old subscriber identity module (“SIM”) cards).

³⁰ See *id.* at 22-24.

in every time CPNI is transferred to any party for any reason. Such rules would be burdensome to carriers and customers alike, would impose notification requirements far beyond the data brokerage and pretexting incidents that gave rise to this inquiry, and are so broad as to disrupt preexisting rules crafted for specific situations.

The Commission should not require carriers to inform customers of the identity of every affiliate, agent, or entity to which the customer's CPNI has been disclosed for marketing purposes. As T-Mobile previously has explained, this issue is unrelated to the data brokering and pretexting incidents at the heart of this proceeding. Moreover, the Commission's new customer notification requirements adopted in the *New CPNI Order* have not even taken effect yet. Expanding these recently promulgated rules is unnecessary and would be counterproductive.

III. CONCLUSION.

The record in this proceeding overwhelmingly supports a cautious and measured approach to further regulation of CPNI. The Commission and Congress have already taken significant steps to protect customer privacy in the *New CPNI Order* and the TRPPA. These two important steps, combined with the considerable customer service and privacy protection efforts

voluntarily undertaken by carriers, are sufficient to meet the Commission's goals. T-Mobile urges the Commission to refrain from additional regulation at this time.

Respectfully submitted,

William F. Maher, Jr.
Joan E. Neal
Alison A. Minea*
MORRISON & FOERSTER LLP
2000 Pennsylvania Ave., N.W.
Washington, D.C. 20006-1888
202.887.1500

Attorneys for T-Mobile USA, Inc.

/s/ Thomas J. Sugrue
Thomas J. Sugrue
Vice President Government Affairs

/s/ Kathleen O'Brien Ham
Kathleen O'Brien Ham
Managing Director, Federal Regulatory
Affairs

/s/ Sara F. Leibman
Sara F. Leibman
Director, Federal Regulatory Affairs

/s/ Shellie Blakeney
Shellie Blakeney
Corporate Counsel, Federal Regulatory
Affairs
T-Mobile USA, Inc.
401 9th Street, N.W.
Suite 550
Washington, D.C. 20004

Dated: August 7, 2007

dc-497368

* Admitted in Maryland, not admitted in D.C.; supervised by attorneys admitted in D.C.