

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

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996:)	
)	CC Dkt. No. 96-115
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;)	
)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	
)	

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

Dated: June 2, 2006

TABLE OF CONTENTS

	Page
I. INTRODUCTION.....	1
II. THE COMMISSION SHOULD FOCUS ON THE DATA BROKER PROBLEM WHILE ACCOMMODATING CUSTOMERS’ DESIRE FOR EXCELLENT SERVICE FROM THEIR CARRIERS	3
III. THE RECORD INDICATES THAT THE COMMISSION SHOULD TAKE REASONABLE STEPS TO IMPROVE ITS OVERSIGHT OF CPNI.....	4
A. The Record Shows That The Annual CPNI Certifications Can And Should Be Improved.....	5
B. The Record Demonstrates That The Measures Proposed In The EPIC Petition And Others In The NPRM Should Not Be Adopted Based On Any Reasonable Policy Analysis	6
C. If The Commission Believes It Necessary To Impose Any Additional Rules, It Should Establish A Set Of Voluntary Practices That Would Constitute A Safe Harbor From Enforcement.....	10
IV. CONCLUSION	11

SUMMARY

The extensive record in this proceeding makes abundantly clear that carriers throughout the telecommunications industry have taken their responsibility to protect CPNI very seriously. The record shows that carriers have taken individualized approaches to implementing a variety of stringent safeguards to protect their customers, while still focusing upon efficient customer service as the market demands.

There is some consensus in the record for further measures that the Commission should take with respect to the annual certification process in order to improve its oversight of CPNI and to increase consumer awareness of the measures that carriers are taking to protect CPNI. Specifically, many parties support an annual FCC filing requirement, and T-Mobile believes that its approach (i.e., requiring annual certification filings within a certain time after the end of a carrier's fiscal year) is the most reasonable means of doing so. Many parties also support the inclusion of certain additional information, such as that suggested by CTIA, in the CPNI certificates or accompanying statements.

The record compiled to date does not justify adoption of the proposals in the EPIC Petition. These proposals – for mandatory passwords, specific audit trail requirements, mandatory encryption, limits on data retention, and new notice requirements – would be costly to implement while hampering law enforcement activities. Further, the record does not show that these proposals, if implemented, would combat the data broker problem.

If the Commission believes additional rules are necessary, however, several commenters support the establishment of safe harbor guidelines from enforcement against inadvertent disclosure of CPNI to data brokers.

The oversight advocated by T-Mobile – implemented flexibly and on an individualized basis by carriers – would allow telecommunications carriers to efficiently and effectively serve their customers while still adequately protecting their privacy. Such an approach will allow carriers to balance their risks and intended permissible uses of CPNI with their customers’ needs and preferences, while still leaving sufficient flexibility to respond to new risks or threats. The Commission should use this opportunity to improve its oversight of CPNI practices in a way that is directly responsive to the data broker problem, without imposing wide-ranging but unrelated and expensive regulations that do not solve the problem at hand.

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

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996:)	
)	CC Dkt. No. 96-115
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;)	
)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	

REPLY COMMENTS OF T-MOBILE USA, INC.

I. INTRODUCTION

In reply to comments on the above-captioned notice of proposed rulemaking (“NPRM”), T-Mobile USA, Inc. (“T-Mobile”) urges the Commission to consider customers’ needs for prompt and convenient service as it considers how best to protect customer proprietary network information (“CPNI”).¹ The NPRM responded to two recent developments in the CPNI area:

¹ T-Mobile holds licenses covering more than 275 million people in 46 of the top 50 U.S. areas and currently serves more than 21.7 million customers. Via its HotSpot service, T-Mobile also provides Wi-Fi (802.11b) wireless broadband Internet access in more than 6700 convenient public locations, such as Starbucks coffee houses, airports, and airline clubs, making it the largest carrier-owned Wi-Fi network in the world.

the petition for rulemaking filed by the Electronic Privacy Information Center² and the fraudulent actions of website data brokers that advertise the availability and sale of individual customer phone records. The NPRM asked whether revisions to the existing CPNI rules are warranted in light of these developments.

The extensive record in this proceeding makes abundantly clear that carriers throughout the telecommunications industry have taken their responsibility to protect CPNI very seriously. The record shows that carriers have implemented a variety of stringent safeguards and sought to close down the data brokers, while still focusing upon efficient customer service. T-Mobile has continued such efforts. Since filing its comments in this proceeding,³ T-Mobile has expanded its aggressive legal actions against data brokers, most recently obtaining an additional injunction against AccuSearch, and obtaining a final order and judgment against Data Find.⁴ T-Mobile also has won additional accolades for its customer service from J.D. Power and Associates.⁵

² Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Dkt. No. 96-115 (filed Aug. 30, 2005) (“EPIC Petition”).

³ Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, CC Dkt. No. 96-115, Comments of T-Mobile USA, Inc. (filed April 28, 2006) (“T-Mobile Comments”). All comments filed in the initial comment cycle in this proceeding will hereinafter be short cited in this manner.

⁴ *T-Mobile USA, Inc. v. AccuSearch*, King County Superior Court, Case No. 06-2-06933-1 SEA (Stipulated Order of Injunction) (filed May 18, 2006); and *T-Mobile USA, Inc. v. 1st Source Info. Serv.*, King County Superior Court, Case No. 06-2-03113-0 SEA (Final Order and Judgment) (May 22, 2006). In addition, on April 28, 2006, T-Mobile sent a second cease and desist letter to Atlas Information Research, Inc. d/b/a atlasresearchusa.com and has since received confirmation of compliance from Atlas.

⁵ T-Mobile Press Release, *T-Mobile Once Again Achieves Highest Honors in Wireless Retail Service* (May 4, 2006), available at <http://t-mobile.com/Company/PressReleases.aspx> (announcing that T-Mobile ranked “Highest in Overall Customer Satisfaction with Wireless Retail Service” in J.D. Power and Associates 2006 Wireless Retail Sales Satisfaction Performance Study); *see also* Candace Heckman, *T-Mobile’s* (Footnote continues on next page.)

There is some consensus in the record for further measures that the Commission should take with respect to the annual certification process in order to improve its oversight of CPNI and to increase consumer awareness of the measures that carriers are taking to protect CPNI.

However, the record compiled to date does not justify adoption of the proposals in the EPIC Petition. Those proposals do not directly address the data broker problem, while being costly to implement and hampering law enforcement activities. In addition, several commenters agree that the Commission should consider establishing safe harbor guidelines from enforcement against inadvertent disclosure of CPNI to data brokers and others committing fraud.

The flexible oversight advocated by T-Mobile would allow telecommunications carriers to efficiently and effectively serve their customers while still adequately protecting their privacy. The Commission should permit such requirements to be implemented flexibly. Accordingly, regulations targeted directly at the data broker problem and taking into consideration customer needs for convenient and efficient service are the issues upon which the Commission should focus its efforts in this proceeding.

II. THE COMMISSION SHOULD FOCUS ON THE DATA BROKER PROBLEM WHILE ACCOMMODATING CUSTOMERS' DESIRE FOR EXCELLENT SERVICE FROM THEIR CARRIERS.

The initial comments in this proceeding show that carriers have taken very seriously their responsibilities to protect CPNI under Section 222 of the Act and the Commission's implementing rules.⁶ Many carriers detailed an array of carefully crafted, stringent safeguards

(Footnote continued from previous page.)

Honesty Earns Satisfaction: Candor With Public Counts, Seattle Post-Intelligencer, May 16, 2006, at C1 (T-Mobile salespeople tell customers when its network will not provide the best wireless service, which resulted in T-Mobile showing the greatest increase among wireless carriers in the American Customer Satisfaction Index).

⁶ See 47 U.S.C. § 222; 47 C.F.R. §§ 64.2001-2009.

that they have adopted in order to meet these responsibilities.⁷ The record also shows that carriers have taken a variety of individualized approaches to implementing appropriate privacy protections and safeguards. However, the safeguards described in the comments reflect, as they must, the need to serve each carrier's customers quickly and efficiently. This is particularly the case in the wireless industry, which continues to be highly competitive and where customers can and do easily switch their wireless service providers. As a result, many of the carriers commenting in this proceeding appropriately highlight customer needs and customer demands in the shaping of their CPNI policies.⁸

In addition, the record makes it clear that carriers have been extremely aggressive in pursuing the data broker industry and supporting tough federal legislation directed against data brokers. In addition to T-Mobile's strong efforts to pursue the data broker lawsuits as described in its comments and as updated above, other carriers have filed numerous lawsuits and dedicated significant resources to targeting the data brokers.⁹

III. THE RECORD INDICATES THAT THE COMMISSION SHOULD TAKE REASONABLE STEPS TO IMPROVE ITS OVERSIGHT OF CPNI.

In addition to the strong actions already taken by carriers to implement stringent safeguards and pursue the illegal data broker industry, the record supports certain additional

⁷ See, e.g., T-Mobile Comments at 5-10; Alltel Comments at 4-5; AT&T Comments at 4-5; BellSouth Comments at 6-9; Cingular Wireless Comments at 4-6; Dobson Comments at 3-5; Eschelon et al. Comments at 3-4; Leap Wireless Comments at 4; MetroPCS Comments at 6-7; and Qwest Comments at 22-34.

⁸ See, e.g., T-Mobile Comments at 4-5, 10-11; Alltel Comments at 2-3; Cingular Wireless Comments at 6-9; Sprint Nextel Comments at 10-11; and Verizon Wireless Comments at 8-9.

⁹ See, e.g., Cingular Wireless Comments at 11-12; Sprint Nextel Comments at 7-8; and Verizon Wireless Comments at 5-7.

steps the Commission should take to improve the annual certification process and to establish safe harbor guidelines. The record also demonstrates that most of EPIC's proposed safeguards are not the type of targeted and rational regulations necessary to solve the data broker problem while still protecting customer interests.

A. The Record Shows That The Annual CPNI Certifications Can And Should Be Improved.

There is some consensus in the record that the annual CPNI certifications can and should be improved. In particular, many parties support an annual filing requirement, although some carriers caution that they must be given sufficient time after the end of the year to carefully review their CPNI compliance in order to ensure that such filings are meaningful.¹⁰ T-Mobile believes that its suggested approach (*i.e.*, requiring annual certification filings within a certain time after the end of a carrier's fiscal year) is the most reasonable of the proposals because it recognizes that carriers may operate on different fiscal years and yet requires filing with the Commission on a consistent schedule.

In addition, some parties supported the inclusion of certain additional information in the CPNI certificates or accompanying statements.¹¹ Upon consideration of the initial comments, T-

¹⁰ See, *e.g.*, T-Mobile Comments at 12-13 (supporting annual filing requirement but suggesting that the deadline be a set date after the end of a carrier's fiscal year); AT&T Comments at 14-15; Cingular Wireless Comments at 14-17; CTIA Comments at 9-11; OPASTCO Comments at 8-9; Qwest Comments at 34-36; Verizon Comments at 8-9; and Verizon Wireless Comments at 18-19.

¹¹ See, *e.g.*, CTIA Comments at 9-11 (certification should include representation that carrier has implemented security procedures to prevent unauthorized CPNI releases and has conducted appropriate training for personnel with CPNI access); and Qwest Comments at 34-36 (certification should include descriptions of hiring practices and controls, authentication procedures, information security controls, and audit capabilities, and should include commitments to offer optional passwords and to retain records only as long as needed for legitimate business purposes).

Mobile supports CTIA's proposal for such additional information, which generally would describe the measures and policies that a carrier has in place. Unlike other suggestions, CTIA's proposal helps increase public awareness and Commission oversight of a carrier's measures to protect CPNI without providing so much detail as to create a "roadmap" for data brokers or others committing fraud.

The Commission should consider implementing CTIA's "beefed-up" annual filing requirement for the CPNI certifications in order to increase the transparency of existing CPNI protections and increase consumer confidence. As T-Mobile and many other parties have stated, however, such certifications should not include annual summaries of legal actions taken against data brokers or summaries of all consumer complaints concerning unauthorized release of CPNI, as such summaries could contain a variety of confidential or competitively sensitive information and would impose substantial burdens while being of limited utility.¹²

B. The Record Demonstrates That The Measures Proposed In The EPIC Petition And Others In The NPRM Should Not Be Adopted Based On Any Reasonable Policy Analysis.

The record demonstrates that the requirements proposed in the EPIC Petition and other potential requirements presented in the NPRM should not be adopted. These requirements are not likely to have any real impact on the data broker problem, but they would impose significant costs and inconvenience on consumers and carriers alike.

For example, customer-set passwords should continue to be optional. The record demonstrates that many carriers already offer optional customer passwords for calls to customer service representatives, but many have decided not to mandate passwords for such inquiries

¹² See, e.g., T-Mobile Comments at 13-14; AT&T Comments at 14-15; Cingular Wireless Comments at 14-17; CTIA Comments at 9-11; and Rural Cellular Association Comments at 5.

based on customer feedback.¹³ Others note that pretexters can fraudulently reset passwords.¹⁴ The Commission should rely upon the experience of carriers in this regard and not mandate passwords for all customer accounts.

Similarly, the record overwhelmingly shows that specific audit trail requirements are far too costly to be required in light of their possible benefit. As commenter after commenter pointed out, audit trails at best will only help to pinpoint and pursue improper disclosures after they have occurred and cannot prevent CPNI disclosures as an initial matter.¹⁵ Further, audit trails would impose very significant costs on carriers that would inevitably be passed through to customers.¹⁶ Accordingly, the Commission should stay the course and follow its earlier decision not to impose such audit trail requirements.¹⁷

¹³ See, e.g., T-Mobile Comments at 11; Alltel Comments at 5; AT&T Comments at 8-11; BellSouth Comments at 15-18; Centennial Comments at 3-4; Charter Comments at 25-28; Cingular Wireless Comments at 19-21; Dobson Comments at 6; Leap Wireless Comments at 5; OPASTCO Comments at 7-8; Qwest Comments at 20-22; Rural Cellular Association Comments at 3; Sprint Nextel Comments at 10-11; Texas Statewide Telephone Cooperative Comments at 3-4; Time Warner Inc. Comments at 10-11; USA Mobility Comments at 12-13; Verizon Comments at 4-8; and Verizon Wireless Comments at 8-9.

¹⁴ See, e.g., Alltel Comments at 5; Eschelon et al. Comments at 5-7; MoPSC Comments at 2-3; Sprint Nextel Comments at 10-11; Time Warner Inc. Comments at 10-11; Time Warner Telecom Comments at 12-13; US LEC Comments at 2-4; and USA Mobility Comments at 12-13.

¹⁵ See, e.g., Alltel Comments at 5-6; CTIA Comments at 14-15; NCTA Comments at 4-5; MoPSC Comments at 3; Rural Cellular Association Comments at 3; Sprint Nextel Comments at 11-13; USA Mobility Comments at 11-12; Verizon Comments at 13-15; and Verizon Wireless Comments at 12-15.

¹⁶ See, e.g., Alltel Comments at 5-6; Charter Comments at 35-36; Cingular Wireless Comments at 21-23 (audit trail would require logging of 380,000 customer contacts per day); Dobson Comments at 6-7 (audit trail would require tracking of 35,000 to 40,000 customer contacts per day); Global Crossing Comments at 4-5; NCTA Comments at 4-5; OPASTCO Comments at 4-5 (audit trail could cost \$1,000 to \$2,000 per access line); Time Warner Inc. Comments at 8-9; Time Warner Telecom Comments at 13-14; USA Mobility Comments at 11-12; Verizon Comments at 13-15 (audit trail would require logging of 400,000 customer calls per

(Footnote continues on next page.)

The Commission should not impose any mandatory encryption requirements on carriers. Instead, it should continue to permit carriers to use encryption flexibly as one of a robust set of “defense-in-depth” methods to protect the confidentiality of their customers’ information. Although the use of encryption can be an effective weapon against some forms of computer and network attack, it does not guarantee that consumer information will be inaccessible to unauthorized individuals. Accordingly, consistent with a flexible regulatory approach, decisions on whether or how to best employ encryption should be left to individual companies and their suppliers.

With respect to possible limits on data retention, numerous parties pointed out the many legitimate uses for such data that would counsel against bright-line limitations – including the resolution of billing disputes or other customer service requests, use in federal or state tax audits, litigation, court-ordered record retention, and response to law enforcement requests, among other uses – and some noted the lack of any evidence that data brokers are attempting to access older information.¹⁸ In light of the many legitimate uses of this data, the potential for conflict with

(Footnote continued from previous page.)

business day); and Verizon Wireless Comments at 12-15 (audit trail could cost \$8 million per year).

¹⁷ *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409 (1999).

¹⁸ *See, e.g.*, AT&T Comments at 16-17; BellSouth Comments at 23-24; Centennial Comments at 5; Charter Comments at 30-32; Cingular Wireless Comments at 24-25; CTIA Comments at 15-16; Eschelon et al. Comments at 8-9; MoPSC Comments at 4; Qwest Comments at 16-18; Sprint Nextel Comments at 15; Time Warner Inc. Comments at 11-12; Verizon Comments at 16-18; and Verizon Wireless Comments at 17-18.

other legal requirements and law enforcement needs,¹⁹ and the lack of any evidence that data brokers are attempting to access older information, the Commission should refrain from imposing any data retention limitations.

In addition, the record demonstrates that Commission adoption of new notice requirements – whether of routine release of information, of breach, or otherwise – is not warranted. As many commenters demonstrated, such notice would be expensive and ineffective, given that the carriers themselves are often not aware of any data broker breach until contacted by the customer, and some forms of notice can be confusing and unduly alarming to customers.²⁰ Accordingly, in light of the fact that carriers already provide customer notice of CPNI breaches pursuant to state law requirements,²¹ and absent solid evidence of the effectiveness of additional notice measures or further guidance from Congress, the Commission should not establish additional notice requirements at this time.

Finally, the record convincingly demonstrates that the elimination of the Commission’s existing “total service approach” to CPNI and opt-out regime is unwarranted. The existing “total service approach,” whereby the Commission reasonably found that customers fully expect

¹⁹ See DOJ/DHS Comments at 2-10 (opposing mandatory data destruction and noting that the benefits of destruction are unclear).

²⁰ See, e.g., Alltel Comments at 5; AT&T Comments at 11-14; BellSouth Comments at 24-26; Charter Comments at 32-35; Cingular Wireless Comments at 25-29; CTIA Comments at 16-18; Dobson Comments at 7-8; Sprint Nextel Comments at 16; Time Warner Inc. Comments at 12-13; Time Warner Telecom Comments at 14; Verizon Comments at 18-20; and Verizon Wireless Comments at 15-17.

²¹ See, e.g., Eschelon et al. Comments at 9-11 (noting that 23 states have notification requirements, and 20 additional states have pending legislation). See also Oklahoma Carriers Comments at 7-8; Qwest Comments at 18-20; Rural Cellular Comments at 3-5; Sprint Nextel Comments at 16; Time Warner Inc. Comments at 12-13; and Verizon Wireless Comments at 15-17.

carriers to use CPNI to market services to them that are within the bounds of the customer-carrier relationship, has struck a reasonable balance in this regard.²² With regard to the opt-out regime, as many parties explained, there is no evidence that third-party partners and contractors (to which opt-out disclosure applies) are the source of any CPNI breaches. More generally, the elimination of the ability to easily outsource certain important functions (such as billing) to third parties would cause great harm to carriers and customers with little corresponding benefit.²³ Accordingly, the Commission should not upset the existing balance that has been struck and approved by the courts with respect to permitting opting-out for certain limited sharing of CPNI.

C. If The Commission Believes It Necessary To Impose Any Additional Rules, It Should Establish A Set Of Voluntary Practices That Would Constitute A Safe Harbor From Enforcement.

Aside from increased requirements relating to the annual CPNI certification, there is no significant consensus in the record regarding additional regulatory obligations to combat the data broker problem. Instead, the record indicates that individualized carrier measures to implement the CPNI rules and to protect the privacy of customers' call records, together with private and governmental enforcement actions and new federal legislation, will best combat the data broker problem without imposing additional, burdensome requirements on consumers and the industry.

If the Commission believes that any additional rules are necessary, however, it should consider the establishment of a set of voluntary practices that would constitute a safe harbor from

²² See, e.g., T-Mobile Comments at 14; Charter Comments at 13-21; and Cingular Wireless Comments at 13-14.

²³ See, e.g., Alltel Comments at 3-4; AT&T Comments at 17-19; BellSouth Comments at 26-32; Charter Comments at 13-21; Cingular Wireless Comments at 13-14; CTIA Comments at 12; Eschelon et al. Comments at 11-16; NTCA Comments at 4; OPASTCO Comments at 6; Time Warner Telecom Comments at 16-18; Verizon Comments at 22-26; and Verizon Wireless Comments at 9-12.

Commission enforcement action against carriers for inadvertent disclosure of CPNI to data brokers or others committing fraud.²⁴ The adoption of these practices could be certified in the annual certification in order to qualify for safe harbor treatment. This type of flexible approach would allow *all* types of carriers to efficiently and cost-effectively serve their customers while still adequately protecting their privacy. This approach would allow carriers to balance their risks and intended permissible uses of CPNI with their customers' needs and preferences, while still leaving sufficient flexibility to respond to new risks or threats.

IV. CONCLUSION

The Commission has a significant opportunity in this docket to reconcile concerns about the protection of CPNI with customer demands for quick, convenient and cost-efficient service from their carriers. The Commission should use this opportunity to improve its oversight of

²⁴ Several carriers proposed some version of voluntary practices to constitute a safe harbor from enforcement. *See, e.g.*, AT&T Comments at 7, n.7; Qwest Comments at 34-36; Verizon Comments at 11-12; and Verizon Wireless Comments at 20-21.

CPNI practices in a way that is directly responsive to the data broker problem, without imposing wide-ranging but unrelated and expensive regulations that do not solve the data broker problem.

T-Mobile looks forward to working with the Commission as it considers these important issues.

Respectfully submitted,

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.

/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/ 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: June 2, 2006