

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

**COMMENTS OF T-MOBILE USA, INC.**

**I. INTRODUCTION**

Pursuant to the Further Notice of Proposed Rulemaking released in the above-captioned proceeding on April 2, 2007 (“FNPRM”), T-Mobile USA, Inc. (“T-Mobile”) hereby comments on the Commission’s proposals for further expanding its rules regarding customer proprietary network information (“CPNI”).<sup>1</sup> T-Mobile strongly supports the goal of protecting the privacy and integrity of customer information and continually develops and implements improved procedures and processes to combat those who attempt to thwart its efforts in this regard. More specifically, T-Mobile endorsed federal legislation to criminalize pretexting and has supported FCC regulation aimed at curtailing pretexting activities. T-Mobile also is moving forward swiftly to implement the Commission’s newly adopted CPNI rules.

---

<sup>1</sup> 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).

T-Mobile nevertheless is concerned about the prospect of additional new CPNI requirements in light of the dramatic changes that already have occurred in the legal and regulatory environment with respect to CPNI in the past several months. Specifically, the FNPRM follows closely on the heels of two recent developments in the CPNI area: (1) the Telephone Records and Privacy Protection Act of 2006 (“TRPPA”), which criminalized pretexting and was signed into law less than six months ago, on January 12, 2007; and (2) the Commission’s sweeping new CPNI regulations, which were released on April 2, 2007, and are not yet in effect.<sup>2</sup> The FNPRM asks whether further expansion of the existing CPNI rules is warranted. Such an expansion of the rules should not even be considered before sufficient time has passed to assess fully the impact of these important recent CPNI developments.

**II. THERE IS NO NEED FOR THE COMMISSION TO FURTHER EXPAND ITS CPNI RULES AT THIS TIME.**

The Commission should allow adequate time to evaluate the effect of the TRPPA and its own recently adopted CPNI requirements before imposing yet more regulation in this area. As the Commission has acknowledged, the TRPPA “should reduce pretexting.”<sup>3</sup> Similarly, the Commission’s rules to contain the pretexting threat, which were imposed on carriers in the *New CPNI Order*, are broad, detailed, and require carriers to undertake major implementation efforts. The public interest would not be served if the Commission moved to impose still more regulations in many of the same areas already considered in the TRPPA and the *New CPNI*

---

<sup>2</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd 6927 (2007), Report & Order and Further Notice of Proposed Rulemaking (2007) (“*New CPNI Order*” or “FNPRM,” as appropriate). All comments and reply comments cited herein refer to comments filed in this proceeding on April 28, 2006, and/or reply comments filed in this proceeding on June 2, 2006, unless otherwise stated.

<sup>3</sup> *New CPNI Order*, 22 FCC Rcd at 6958 n.195.

*Order* without first determining the impact of the newly adopted rules once they actually take effect. As discussed below, the burdens and costs of the FNPRM’s proposed requirements – to customer convenience, to carriers’ operations, and to effective law enforcement – far outweigh any potential benefits to customer privacy.

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

The *New CPNI Order* just imposed rules that require a customer password for call-in access to call detail information (“CDI”).<sup>4</sup> In so doing, the Commission specifically found that, by limiting the rule to the disclosure of CDI, it had appropriately tailored its requirements to address the demonstrated problem of pretexting.<sup>5</sup> Instead of imposing an overly broad requirement that does not directly address protecting the information pretexters seek, T-Mobile urges the Commission to allow sufficient time to assess the effects on customer welfare of its existing password rule.

The record is abundantly clear that customers dislike passwords,<sup>6</sup> including evidence that passwords significantly disrupt customers’ ability to resolve routine billing questions and

---

<sup>4</sup> *Id.* at 6936-39; *see also* 47 C.F.R. § 64.2010(b). The Commission defined CDI as “any information that pertains to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.” *New CPNI Order*, 22 FCC Rcd at 6936 n.45.

<sup>5</sup> *New CPNI Order*, 22 FCC Rcd at 6936 n.46.

<sup>6</sup> *See, e.g., New CPNI Order*, 22 FCC Rcd at 6936 n.47 (“We understand that many consumers may not like passwords....”); T-Mobile Comments at 11 (explaining that T-Mobile at one point required mandatory passwords for call-in access, but changed to optional passwords in response to high customer dissatisfaction); T-Mobile Reply Comments at 6-7 n.13; and AT&T Comments at 8-11 (noting studies that demonstrate customers oppose mandatory passwords). Furthermore, passwords can be difficult or impossible for some customers to use. *See, e.g.,* Comments of the American Association of People With Disabilities, American Council of the Blind, and the National Spinal Cord Injury Association at 1-3 (Dec. 8, 2006).

problems over the telephone without delay or disruption. The significant inconvenience of mandating passwords for non-CDI (or requiring customers to await mailed information or to go to a retail location to obtain CDI) must be weighed against the fact that there is no evidence in the record that data brokers have any interest in non-CDI associated with customer accounts.<sup>7</sup> Accordingly, the Commission should not adopt the FNPRM's proposal to extend the call-in password requirement to non-CDI.<sup>8</sup>

**B. The Record Remains Clear That the Cost of Requiring Audit Trails Far Outweigh Their Consumer Benefits.**

Although the Commission initially adopted an audit trail requirement when first implementing the CPNI provisions of the Telecommunications Act of 1996, the Commission eliminated the requirement in 1999, correctly concluding that the high costs of using audit trails far outweigh any potential consumer benefit.<sup>9</sup> The Commission again raised this issue in 2006, and, as noted in the *New CPNI Order*, the current record echoes the Commission's previous determination "that the broad use of audit trails likely would be of limited value in ending pretexting because such a log would record enormous amounts of data, the vast majority of it being legitimate customer inquiry."<sup>10</sup> However, the FNPRM asks yet again whether the

---

<sup>7</sup> See, e.g., Letter from William F. Maher, Jr., Counsel for T-Mobile, to Marlene H. Dortch, Secretary, FCC at 1-2 (Nov. 30, 2006) (call detail records, not other forms of CPNI, are the main target of pretexters) (also citing letter from Verizon Wireless).

<sup>8</sup> FNPRM, 22 FCC Rcd at 6960-61.

<sup>9</sup> *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) ("*1999 CPNI Order*").

<sup>10</sup> See, e.g., *New CPNI Order*, 22 FCC Rcd at 6961 ("Commenters also report that implementing and maintaining audit trails would be costly with little to no corresponding benefit to the consumer"); T-Mobile Comments at 16; and T-Mobile Reply Comments at 7 n.16.

Commission should impose an audit trail requirement.<sup>11</sup> The Commission should allow its newly adopted rules to operate rather than adopt this unnecessary requirement.

As T-Mobile explained in its 2006 comments,<sup>12</sup> as long ago as 1999 the Commission found credible evidence that the implementation of an audit trail requirement could cost tens of millions of dollars per carrier.<sup>13</sup> As a result, the Commission decided to modify the earlier-ordered audit trail requirement. Because carriers were already obligated to protect CPNI, the Commission concluded “that, on balance, such a potentially costly and burdensome rule does not justify its benefit.”<sup>14</sup>

These conclusions apply with equal validity today. Many carriers already monitor and record customer interactions in some way. A new audit trail requirement could be superfluous or, for carriers with well-established monitoring systems and procedures, could require carriers to modify their existing systems at significant cost.<sup>15</sup> For example, even in the absence of specific requirements, T-Mobile’s customer care systems already create audit logs of access to customer information by customer care representatives to identify the specific representative who initiated any particular transaction.<sup>16</sup> We are also concerned that by disrupting established processes and systems with a new set of requirements, the Commission may inadvertently hinder carriers’ efforts to assist law enforcement agencies in investigating pretexters.

---

<sup>11</sup> FNPRM, 22 FCC Rcd at 6961.

<sup>12</sup> *See* T-Mobile Comments at 16.

<sup>13</sup> *See 1999 CPNI Order*, 14 FCC Rcd at 14472.

<sup>14</sup> *Id.* at 14475.

<sup>15</sup> *See* T-Mobile Comments at 16.

<sup>16</sup> *Id.*

There have been no technological or operational developments in the intervening year since the record leading up to the *New CPNI Order* was compiled that change in any material way the Commission's correct decision in 1999 to eliminate the audit trail requirement, and thus the Commission should again decline to impose such a requirement.

**C. Rules Governing the Physical Transfer of CPNI Among Companies Are Not Warranted at This Time.**

The FNPRM asks if the Commission should adopt rules governing the physical transfer of CPNI among companies, including from carriers to their affiliates and independent contractors or joint venture partners.<sup>17</sup> The examples cited in the FNPRM include requirements for audit trails and encryption – measures the Commission has considered and declined to adopt in this proceeding to date.<sup>18</sup> Such rules could impose major costs on carriers and their customers with minimal corresponding benefit. Instead of burdening carriers and customers with such a requirement, the Commission instead should permit its new rules the opportunity to work.

In addition, there is no evidence cited in the FNPRM that data brokers have been able to circumvent carriers' current systems to obtain CPNI during such a physical transfer. Furthermore, specific rules governing the physical transfer of CPNI could run the risk of providing a "roadmap" or users' manual to data brokers and/or hackers on how to compromise carriers' systems for transferring data. Rather than adopt a potentially harmful and unnecessary rule, the Commission should allow companies the discretion to implement mechanisms that best complement their customer needs and existing systems.

---

<sup>17</sup> FNPRM, 22 FCC Rcd at 6961.

<sup>18</sup> *See, e.g., supra* Section II.B.

**D. The Commission Should Not Adopt New Rules Limiting Data Retention.**

The FNPRM again raises the issue of whether the Commission should adopt rules limiting carriers' data retention.<sup>19</sup> As the 2006 record in this proceeding made clear, such rules would be counter-productive on several levels. First, the Department of Justice and Department of Homeland Security have raised concerns that any such rules adopted by the Commission could significantly hinder important law enforcement efforts.<sup>20</sup> In addition, data retention limits could well conflict with other Commission and state law requirements,<sup>21</sup> as well as individual carrier obligations adopted in national security agreements.<sup>22</sup> Finally, there is no evidence in the record that data brokers are interested in the older information that carriers retain for many legitimate reasons.<sup>23</sup> The Commission therefore should refrain from imposing a data retention limit that could work at cross-purposes with law enforcement needs and carriers' well-established legal and business requirements. Instead, the Commission should permit law enforcement to use its new tool, the TRPPA, to crack down on the data broker industry.

---

<sup>19</sup> FNPRM, 22 FCC Rcd at 6961-62.

<sup>20</sup> *See* DOJ/DHS Comments at 2-10 (stating that mandatory destruction of CPNI would severely impact the ability of DOJ/DHS to protect national security and public safety).

<sup>21</sup> *See, e.g.*, 47 C.F.R. § 42.6 (requiring carriers to retain telephone toll records for 18 months).

<sup>22</sup> *See, e.g.*, T-Mobile Comments at 17 n.42 (stating that T-Mobile is required to retain certain customer records, such as billing information, for a period longer than 18 months pursuant to its national security agreement negotiated with the federal government).

<sup>23</sup> *See, e.g.*, T-Mobile Comments at 17 (noting that, in T-Mobile's experience, data brokers are interested only in current information); T-Mobile Reply Comments at 8 n.18; and Cingular Comments at 24-25 (noting that data brokers appear to focus on last 100 calls or calls within last 90 days).

**E. The Commission Should Not Impose New Carrier Requirements Regarding The Protection of Information Stored in Mobile Communications Devices.**

The FNPRM asks if the Commission should consider new rules regarding the protection of information stored in mobile communications devices.<sup>24</sup> T-Mobile agrees that the ability to delete such data is important for customer privacy. Mobile handsets used in providing T-Mobile's services, however, generally already have such deletion capability, and T-Mobile's public website provides instructions and guidance to customers on how to delete or erase personal data from their handsets prior to discarding or refurbishing such devices.<sup>25</sup> T-Mobile sales and customer care representatives are also on hand to provide assistance to subscribers desiring to delete such information. Consumers are becoming more sensitized to the need to protect the privacy of information they choose to store on their handsets, and carriers and manufacturers have responded to their demands through the development of improved handset capabilities as well as online, phone and in-person customer assistance. Specific rules in this area are unlikely to be as technologically advanced or responsive to customer needs as the measures already undertaken – and continually improved – by the industry.

---

<sup>24</sup> FNPRM, 22 FCC Rcd at 6962.

<sup>25</sup> See T-Mobile.com, *How Can I Delete Data from My Device?*, <http://support.t-mobile.com/knowledge/root/public/tm20506.htm#all> (last visited July 5, 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](http://www.t-mobile.com/Company/Community.aspx?tp=Abt_Tab_HandsetRecycling) (last visited July 5, 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/knowledge/root/public/tm23344.htm> (last visited July 5, 2007) (explaining how to delete data on old subscriber identity module ("SIM") cards).

### III. CONCLUSION.

Although T-Mobile strongly supports and shares the Commission's goals of protecting customers' CPNI, T-Mobile cautions against the adoption of additional burdensome and likely counterproductive regulation. Rather, the Commission should allow sufficient time to assess the impact of the TRPPA and the Commission's own rules adopted in the *New CPNI Order*. Only if the Commission determines that these measures have been ineffective or insufficient should the Commission consider imposing further regulations that will impose additional costs on consumers and carriers alike.

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.

Respectfully submitted,

/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 9<sup>th</sup> Street, N.W.  
Suite 550  
Washington, D.C. 20004

Dated: July 9, 2007

dc-493817