

**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

**COMMENTS OF COMCAST CORPORATION**

**I. INTRODUCTION AND SUMMARY**

Comcast Corporation (“Comcast”) submits these comments in response to the above-captioned Further Notice of Proposed Rulemaking (“Further Notice”).<sup>1</sup> Comcast, through its various subsidiaries, is a provider of both interconnected Voice over Internet Protocol (“VoIP”) service and circuit-switched service. In its Further Notice, the FCC seeks comment on what additional steps, if any, it should take to secure further the privacy of customer proprietary network information (“CPNI”). Specifically, the FCC asks whether it should adopt any further requirements regarding password protection, audit trails, physical safeguards or data retention. As discussed below, these additional proposed measures are unnecessary and would impose burdens on consumers that far outweigh any asserted benefits. The Commission, therefore, should take no further action in this proceeding. At a minimum, it should defer any further

---

<sup>1</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (FCC 07-22).

action until its latest CPNI rules, released only three months ago, have been fully implemented and there has been an opportunity to evaluate their effectiveness.

## **II. ARGUMENT**

### **A. Comcast Has Implemented a Comprehensive Plan to Prevent the Unauthorized Disclosure of CPNI**

Comcast has a long-standing policy of developing and implementing a variety of safeguards to ensure the security of CPNI in its possession. Among other things, Comcast establishes, documents and maintains internal processes and controls, including audits and supervisory reviews, to ensure compliance with CPNI rules. Comcast also strictly limits in-house and vendor employee access to CPNI to those individuals who need to use CPNI in order to perform their duties (*e.g.*, customer care personnel who handle consumer inquiries about their bills). Before these individuals are permitted access to CPNI, they first receive training regarding the FCC's CPNI regulations, including the following topics:

- The definition of CPNI and Comcast's CPNI policies;
- The process for verifying or changing a customer's CPNI settings;
- Proper (and improper) use and disclosure of a customer's CPNI;
- Potential consequences of improper use or disclosure of CPNI, including disciplinary actions up to and including termination of employment; and
- Procedures to follow in the event that an individual becomes aware of an unauthorized disclosure of CPNI.

In addition, employees are required to pass a test at the conclusion of the training session before they are permitted to gain access to CPNI in Comcast's possession.

All managers who supervise individuals having access to CPNI similarly must complete introductory and management-level CPNI training as well as demonstrate familiarity with the

information in Comcast's CPNI Compliance Manual. Comcast also designates certain key management personnel to serve as Designated Compliance Officers ("DCO"), who are responsible for helping to oversee the company's CPNI compliance effort. In addition to a Chief DCO at the corporate level, there is one division-level DCO at each of Comcast's Atlantic, Mid-West, North Central, Southern and Western Divisions.

Comcast also takes steps to ensure that its customers stay informed about its CPNI policies. Comcast provides all new customers with a copy of its privacy policy, including CPNI policies for Comcast Digital Voice and Comcast Digital Phone, in their welcome kits. Existing customers receive copies of the policy annually thereafter. The policy is also continuously posted online at <http://www.comcast.com/customerprivacy/>.

Comcast obtains, verifies, and records customer preferences regarding use of CPNI for purposes of marketing telecommunications and non-communications-related services. It is currently not Comcast's practice to share CPNI with its marketing partners, and DCO approval is required for the use of CPNI in any and all Comcast marketing campaigns. In those cases in which it does transfer CPNI (*e.g.*, to vendors who handle consumer inquiries or produce bills), Comcast either encrypts the data and/or transmits it over a secure (dedicated) transmission channel. Comcast also conducts semiannual internal certifications of its compliance with FCC CPNI rules and keeps its certification of compliance with those rules on public file. These safeguards will be augmented by the additional requirements imposed by the FCC in the April 2, 2007 Report and Order.<sup>2</sup>

---

<sup>2</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order, 22 FCC Rcd 6927 (2007) (FCC 07-22) ("Report and Order").

**B. The Additional CPNI Measures Mentioned in the Further Notice Are Unnecessary and Would Impose Burdens on Consumers that Far Outweigh Any Asserted Benefits**

As many commenting parties pointed out in response to the prior Notice,<sup>3</sup> the Commission's adoption of the additional CPNI measures outlined in the Further Notice will lead to increased customer frustration and confusion while providing little or no additional deterrence to pretexters seeking to obtain unauthorized access to customers' call detail records. The FCC, therefore, should decline to adopt these additional CPNI measures. At a minimum, the Commission should defer any further action in this proceeding until the CPNI requirements released just three months ago have been implemented and their effectiveness evaluated.

**1. Passwords**

The FCC should not extend password requirements to all CPNI for customer-initiated telephone calls nor apply such requirements to customer-initiated account changes. Extending the password requirement to other customer-initiated contacts clearly would cause greater inconvenience and confusion for Comcast consumers and would provide little additional protection against the unauthorized disclosure of CPNI.

In Comcast's experience, most customer issues relate to billing. Therefore, these issues likely also account for the bulk of customer-initiated telephone inquiries that Comcast receives. For example, a consumer whose bill has been misplaced or lost in the mail may call to ask for the total amount due in order to arrange payment. Or a consumer may have a question about the tax calculation on his or her bill or the rate plan in which he or she is enrolled. Months or even years frequently may pass between inquiries from the same individual consumer. If the FCC extended the password requirement as suggested in the Further Notice, the consumer would be required to

---

<sup>3</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, 21 FCC Rcd 1782 (2006) ("Notice").

provide his or her password upon each and every contact before Comcast could respond to routine questions about the consumer's bill that do not involve call detail. Requiring customers to obtain and remember passwords from one ordinary billing inquiry to the next not only would prevent companies like Comcast from efficiently responding to its customers' needs, but also would needlessly confuse and frustrate customers. Consumers who choose to obtain access to their billing information through Comcast's online service, of course, already must provide a password in order to review even routine information. Consumers who prefer to call Comcast's customer service number, however, may access our online service less frequently or may lack Internet access altogether and, hence, are likely less familiar and comfortable with mandatory password requirements. For such consumers, extending password requirements to routine billing information would create an unnecessary obstacle.

In its Report and Order, the Commission asserts that the "ongoing burdens of these [call detail] authentication requirements will be minimal and are outweighed by the benefits to consumer privacy."<sup>4</sup> Comcast disagrees, particularly with respect to records that do not involve call detail. The percentage of customer-initiated calls to companies like Comcast that would be subject to the requirement would skyrocket, leading to longer customer service call times, delayed access to information, and increased customer dissatisfaction. Further, as noted, many customer-initiated calls involve billing or other routine account inquiries, the vast majority of which do not implicate the pretexting problem the Commission is seeking to address through these requirements.

The new notice requirements adopted in the Report and Order adequately protect consumers against pretexter abuse. Pursuant to those rules, carriers must notify the customer of record (either at the telephone or address of record) whenever (1) a password, (2) a back-up authentication question (*e.g.*, "what was your first pet's name?"), (3) an online account, or (4) the

---

<sup>4</sup> Report and Order ¶ 22.

address of record is created or changed.<sup>5</sup> Thus, for example, if a pretexter were able to change the address of record during a telephone-initiated contact or change the password online, the carrier would notify the customer immediately.<sup>6</sup> As the FCC recognized, this requirement will alert the customer to an unauthorized change and enable the customer and carrier to take appropriate action.<sup>7</sup> Given the consumer costs of extending this requirement to mundane bill inquiries, the Commission should decline to do so. At a minimum, it should defer any further action in this proceeding until its initial CPNI rules have been implemented and their effectiveness evaluated.

## 2. Audit Trails

As the Commission acknowledged in the Further Notice, the record in this docket demonstrates that the 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>8</sup> Moreover, an “electronic audit trail requirement would generate ‘massive’ data storage requirements at great cost”<sup>9</sup> and ironically could compromise customer privacy by requiring carriers to collect and maintain vast amounts of data that they otherwise

---

<sup>5</sup> Report and Order ¶ 24.

<sup>6</sup> In addition, the new rules make it harder for pretexters successfully to change the address of record for the purpose of being sent call record details, because an address of record must have been associated with the customer’s account for at least 30 days. Report and Order ¶ 13 n.46.

<sup>7</sup> Even if the FCC, *arguendo*, were to extend the password requirement, it should continue to exempt routine customer-initiated inquiries regarding their bills so long as the customer is able to provide the carrier all of the necessary call detail information. Maintaining this exemption will continue to ensure that providers are able to handle routine customer bill inquiries without unnecessarily antagonizing customers.

<sup>8</sup> Further Notice ¶ 69.

<sup>9</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, ¶ 127 (1999) (“1999 Reconsideration Order”) (quoting AT&T).

would not in the ordinary course of business. Commenters also previously have pointed out that if a pretexting incident occurred, an audit trail likely would “only indicate that the customer made an inquiry and successfully authenticated himself/herself at a given date and time.”<sup>10</sup>

The FCC in 1999 adopted and then rescinded an audit trail requirement, concluding that the substantial burden and cost (estimated by one carrier to be \$270 million for that carrier alone) outweighed any perceived benefit.<sup>11</sup> Nothing has changed that would justify a different conclusion. If anything, the cost of complying with an audit trail requirement would undoubtedly be higher today than in 1999.

### **3. Physical Safeguards**

The Further Notice seeks comment on the types of physical safeguards carriers currently employ when transferring or allowing access to CPNI by the carrier, its affiliates or other authorized third parties. The Notice also asks whether it should adopt rules that govern the physical transfer of or access to CPNI, such as requiring encryption.<sup>12</sup>

As described earlier, Comcast already has implemented comprehensive policies and procedures that protect against unauthorized access to CPNI, restrict internal access to CPNI, and ensure the secure transfer of its CPNI to third parties. Among other things, Comcast strictly limits access to CPNI to those individuals who require access to perform their job duties. These personnel receive extensive training concerning the proper handling of CPNI and are subject to disciplinary measures, including termination, for breaches of Comcast’s CPNI procedures. It is

---

<sup>10</sup> Sprint Nextel Reply Comments at 9 (filed June 2, 2006); *see also* Time Warner Telecom Comments at 13 (filed April 28, 2006). (Comments cited herein were filed in CC Docket No. 96-115.)

<sup>11</sup> 1999 Reconsideration Order ¶¶ 124, 127.

<sup>12</sup> Further Notice ¶ 70. The only other physical safeguards expressly mentioned in the Further Notice are audit trails and logs. These requirements should be rejected for the reasons set forth in section II.B.2, *supra*.

currently not Comcast's practice to share CPNI with its marketing partners, and, in those limited circumstances in which it does transfer CPNI, Comcast either encrypts the data and/or transmits it over a secure (dedicated) transmission channel.

Requiring carriers to encrypt all CPNI data – regardless of other physical safeguards in place – would be prohibitively expensive and offer only modestly (if any) greater protection against pretexters. Indeed, the Commission itself previously has conceded that there is no record evidence that pretexters have obtained access to CPNI by “hacking” into carrier databases.<sup>13</sup> Carriers already have a duty to protect CPNI stored in their databases.<sup>14</sup> Encryption is but one among several technologies that permit carriers to protect their customers' sensitive information. Rather than dictating “one size fits all” encryption requirements or other physical safeguards, the Commission should instead continue to permit providers to determine appropriate measures for safeguarding access to and transfer of CPNI, based upon their particular circumstances. In today's competitive voice marketplace, the protection of customers' proprietary information is not only a matter of security but also a matter of building consumer trust and confidence. Providers will voluntarily implement necessary protective measures regarding customers' CPNI because, without those measures, the providers' service would not be viable in the marketplace.

#### **4. Data Retention**

The Further Notice asks whether the Commission should limit the duration of the period that a carrier may retain CPNI. The answer to that question is plainly “no,” because it would interfere with the ability of Comcast and other providers to manage their businesses efficiently.

VoIP and circuit-switched voice service providers are potentially subject to a variety of laws that may conflict with any mandatory CPNI data retention requirement. FCC rules, for

---

<sup>13</sup> Report and Order ¶ 36.

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

example, require providers to retain for the duration of service Lifeline/Link-up certificates of eligibility<sup>15</sup> and VoIP E911 acknowledgments.<sup>16</sup> Contributors to universal service are required to maintain the records and underlying documentation necessary to justify information reported in their Telecommunications Reporting Worksheet for three years after the date the worksheet is due.<sup>17</sup>

Voice service providers often need to retain customer records for state and federal legal, business, and tax purposes. For example, Comcast frequently needs access to historic CPNI in connection with disputes or litigation involving customer bills. In some cases, these disputes or litigation may drag on for years. Comcast also requires access to historic billing data for tax audits.

To the extent that the FCC were to adopt a mandatory data retention requirement that is shorter than these other intervals, Comcast would be placed in an untenable position of attempting to comply with conflicting legal requirements.

The Commission also seeks comment on whether it should require carriers to “de-identify” customer records after a certain period of time.<sup>18</sup> Because de-identification would erase the call detail in a customer’s record, a mandatory requirement to de-identify CPNI by a date certain would raise essentially the same issues as a mandatory destruction requirement. De-identified data would be useless to law enforcement agencies seeking to track a suspect’s calls on a particular day, or to match a tax exemption certificate with a particular account in connection

---

<sup>15</sup> 47 CFR § 54.417(a).

<sup>16</sup> 47 CFR § 9.5(e).

<sup>17</sup> 47 CFR 54.711(a).

<sup>18</sup> Further Notice ¶ 71.

with a tax audit. De-identifying data would also be time-consuming and expensive to implement.

### III. CONCLUSION

For the foregoing reasons, the Commission should conclude that existing CPNI regulations are more than sufficient to secure the privacy of customer information, and that additional safeguards are not required.

Respectfully submitted,

Joseph W. Waz  
COMCAST CORPORATION  
1500 Market Street  
Philadelphia, PA 19102

James R. Coltharp  
Mary P. McManus  
COMCAST CORPORATION  
2001 Pennsylvania Avenue, Suite 500  
Washington, DC 20006

Brian A. Rankin  
Beth A. Choroser  
Samuel F. Cullari  
COMCAST CABLE COMMUNICATIONS, LLC  
1500 Market Street  
Philadelphia, PA 19102

/s/ A. Richard Metzger, Jr.  
A. Richard Metzger, Jr.  
A. Renée Callahan  
LAWLER, METZGER, MILKMAN & KEENEY, LLC  
2001 K Street, NW, Suite 802  
Washington, DC 20006  
(202) 777-7700  
*rcallahan@lmmk.com*

July 9, 2007

## Certificate of Service

I hereby certify that on this 9th day of July 2007, I caused true and correct copies of the foregoing Comments of Comcast Corporation to be mailed by electronic mail to:

Janice Myles  
Competition Policy Division  
Wireline Competition Bureau  
Federal Communications Commission  
445 12th Street SW, Room 5-C140  
Washington, DC 20554  
janice.myles@fcc.gov

Best Copy and Printing, Inc.  
445 12th Street SW, Room CY-B402  
Washington, DC 20554  
fcc@bcpiweb.com

/s/ Ruth E. Holder  
Ruth E. Holder