

**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 CHARTER COMMUNICATIONS, INC.**

Christin S. McMeley  
Vice President & Senior Counsel  
Deputy Compliance Officer  
Charter Communications, Inc.  
12405 Powerscourt Drive  
St. Louis, MO 63131

Christopher Wolf  
Timothy P. Tobin  
Proskauer Rose LLP  
1001 Pennsylvania Avenue, N.W.  
Suite 400 South  
Washington, D.C. 20004-2533

Attorneys for Charter  
Communications, Inc.

August 7, 2007

## SUMMARY

Further amendments to the Commission's CPNI rules would be unnecessary and unwise. The Commission's CPNI rules as just supplemented by the Commission are already extensive. Moreover, this new, far-reaching regime has not yet taken effect; there has been no opportunity to assess the effectiveness or the impact of the additional requirements. It is clear, however, that the additional measures discussed in the Commission's further notice of proposed rulemaking would not appreciably decrease pretexting or help secure CPNI. Instead, they would serve only to increase the costs on carriers and therefore consumers. Likewise, other additional proposals advocated by coalition of groups would also not benefit consumers and would only serve to raise costs and complicate carrier operations. All of these proposals are therefore overbroad. They would unnecessarily interfere with carriers' ability to communicate with their customers and to that extent, they violate the First Amendment.

The Commission should be aware of other reasons that render additional rules unnecessary. Congress's recent criminalization of pretexting for phone records provides a significant deterrent to those who would otherwise engage in pretexting. Moreover, in the competitive environment for telecommunications services that exists today, carriers already have incentives to protect their customers' privacy. If they fail to do so, carriers risk customer loss and damage to share price and reputation. Because every carrier's business is structured differently, carriers should have the flexibility to adopt security practices that are reasonable for their individual circumstances. They should not be subject to broad mandates such as those proposed in the further notice of proposed rulemaking or other proposed rules that would ultimately do more harm than good.

## TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	BECAUSE OF THE FAR-REACHING RULES THE COMMISSION HAS ALREADY ADOPTED AND COMPETITIVE PRESSURES, ADDITIONAL NEW RULES ARE UNNECESSARY.....	2
	A. The Commission’s Newly Supplemented Rules Are Already Extensive.....	2
	B. Competitive Pressures Also Make New Rules Unnecessary.....	4
III.	THE CONSUMER COALITION’S ARGUMENTS IN SUPPORT OF THE ISSUES RAISED IN THE NPRM ARE NOT PERSUASIVE.....	7
	A. Mandating Password Protection for Non-Call Detail CPNI Would be Ill-Advised.....	7
	B. The Costs of Audit Trails Outweigh the Consumer Benefits .....	9
	C. Specific Mandates for Physical Safeguards are Unnecessary.....	11
	D. Limiting Data Retention Would Be Complex and Unworkable .....	13
IV.	THE CONSUMER COALITION’S “ADDITIONAL RECOMMENDATIONS” ARE ILL-ADVISED.....	15
	A. Eliminating the Law Enforcement Delay Provision Could Harm Investigations .....	15
	B. Requiring Opt-In for All Sharing of CPNI is Bad Policy and Violates the First Amendment .....	16
V.	CONCLUSION.....	19

**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 CHARTER COMMUNICATIONS, INC.**

**I. INTRODUCTION**

Charter Communications, Inc. (“Charter” or the “Company”) submits these reply comments in opposition to the Commission’s proposed adoption of additional rules as set forth in the further notice of proposed rulemaking in the above captioned dockets.<sup>1</sup> Charter is a broadband communications provider with operations in 30 states. In many of its service areas, Charter offers voice services, primarily through interconnected Voice over Internet Protocol (“VoIP”) technology in addition to other advanced broadband services, including traditional cable video programming (both analog and digital) and high-speed cable Internet access, over its broadband networks.

As amply demonstrated in the comments submitted in response to the *FNPRM*, amending the rules again is unnecessary and unwise. The extensive amendments to CPNI rules the

---

<sup>1</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115, WC Docket No. 04-36, FCC 07-22 (rel. Apr. 2, 2007) (“*Report and Order*” or “*FNPRM*”).

Commission recently adopted in the *Report and Order* have not yet even taken effect and there has been no opportunity to assess the effectiveness or the impact of those additional requirements. Judging by the paucity of comments in support of additional supplemental rules, consumers agree that the rules as amended by the *Report and Order* are sufficient.<sup>2</sup> Moreover, the primary set of comments in support of even more changes to the rules, filed by a coalition of groups led by the Electronic Information Privacy Center (“EPIC”), collectively the “Consumer Coalition,” do not make the case for additional rules.

The Consumer Coalition, in advocating for the measures discussed in the *FNPRM*, ignores the reach of the Commission’s recently adopted regime and the effect of the recently enacted federal law criminalizing pretexting, disregards the costs to carriers and consumers, and fails to acknowledge the significant additional pressures carriers have to protect CPNI.

**II. BECAUSE OF THE FAR-REACHING RULES THE COMMISSION HAS ALREADY ADOPTED AND COMPETITIVE PRESSURES, ADDITIONAL NEW RULES ARE UNNECESSARY.**

**A. The Commission’s Newly Supplemented Rules Are Already Extensive**

As the Commission has reiterated, carriers are already under a longstanding obligation, established in the Telecommunications Act of 1996, to “protect the confidentiality of proprietary information ... of customers.”<sup>3</sup> That obligation is fundamental. It required, and continues to require, carriers to take reasonable steps to protect CPNI. As Charter explained in its comments in response to the Commission’s 2006 notice of proposed rulemaking,<sup>4</sup> that duty has long been

---

<sup>2</sup> In stark contrast to the initial comments filed last year in response to the notice of proposed rulemaking, which included numerous comments supporting expanded rules, for the *FNPRM*, there were only two sets of comments filed in support of expanding CPNI rules further.

<sup>3</sup> 47 U.S.C. § 222(a); *Report and Order* ¶¶ 6, 20, 35.

<sup>4</sup> *Implementation of the Telecommunications Act of 1996: 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*

supplemented by a host of Commission CPNI rules,<sup>5</sup> which has included requiring carriers to establish a system to track customer approval for use of CPNI,<sup>6</sup> training personnel and instituting a disciplinary process,<sup>7</sup> maintaining records of carriers' and affiliates' use of CPNI for marketing campaigns and disclosures to third parties,<sup>8</sup> requiring supervisory review of outbound marketing campaigns,<sup>9</sup> requiring an officer to sign an annual compliance certificate,<sup>10</sup> and mandating oversight of independent contractor or joint venture partners.<sup>11</sup> The measures discussed in the *FNPRM* will not substantially strengthen CPNI protections and will serve only to impose extra costs on carriers, which ultimately will harm consumers.

Only four months ago, the Commission adopted a wide ranging set of additional rules that, in combination with those already in place, establish a far-reaching regulatory regime intending to heavily protect CPNI. This new regime with its authentication and password requirements, customer and law enforcement notification mandates, and opt-in consent for sharing of CPNI for marketing to carrier's joint venture partners/independent contractors, among others, in many instances requires carriers to make significant modifications to their practices. As Time Warner aptly explained in its *FNPRM* comments, “[t]he breadth and depth of the Commission’s regulatory regime and these multifaceted enforcement tools provide a compelling

---

*Proprietary Network Information*, Notice of Proposed Rulemaking, CC Docket No. 96-115, FCC 06-10 (rel. Feb. 14, 2006) (“*NPRM*”).

<sup>5</sup> See Charter Comments, at 6 (Apr. 28, 2006) (“Charter *NPRM* Comments”).

<sup>6</sup> 47 C.F.R. § 64.2009(a).

<sup>7</sup> *Id.* at § 64.2009(b).

<sup>8</sup> *Id.* at § 64.2009(c).

<sup>9</sup> *Id.* at § 64.2009(d).

<sup>10</sup> *Id.* at § 64.2009(e).

<sup>11</sup> *Id.* at § 64.2007(b)(2).

argument against adopting even more regulation.”<sup>12</sup> Moreover, Congress only recently criminalized phone record pretexting.<sup>13</sup> Enforcement of that and similar state laws would be the single biggest contributor to the security of CPNI, serving as a significant deterrent to pretexting. Given these factors, additional new rules are not necessary to protect CPNI and would be ill advised.

### **B. Competitive Pressures Also Make New Rules Unnecessary**

The Consumer Coalition ignores the competitive incentives that carriers have to protect privacy. That incentive arises from the intense competition for telecommunications services that exists nationwide and it leads carriers to search for ways to distinguish themselves to consumers. In such an environment, missteps in protecting customer privacy are subject to punishment in the marketplace. Charter, in its comments filed in response to the NPRM last year, explained the competitive pressures on carriers to protect CPNI.<sup>14</sup> Charter cited studies supporting that conclusion, including one demonstrating that nearly 20 percent of customers immediately terminate service with companies that have lost their personal information and an additional 40 percent of customers consider terminating their relationship with such companies.<sup>15</sup> In other words, nearly 60 percent of consumers either immediately terminate or consider switching or dropping a provider based on that company’s failure to adequately protect personal information.<sup>16</sup> In addition to customer loss, the marketplace also punishes businesses by directly

---

<sup>12</sup> See Time Warner FNPRM Comments, at 5 (July 9, 2007).

<sup>13</sup> See Telephone Records and Privacy Protection Act, Pub. L. No. 109-476, 120 Stat. 3568 (2007).

<sup>14</sup> Charter NPRM Comments, at 7-9.

<sup>15</sup> *Id.* at 8, n.24 (citing *Survey: Data Losses Spur Consumer Flight*, CIO Today, Jan. 27, 2006, which cited survey conducted by Ponemon Institute Study and distributed by PGP Corp.).

<sup>16</sup> *Id.* at 8. Similar findings were made for customers of banks and other financial institutions. See Gene J. Koprowski, *Survey: Consumers Inclined to Switch Banks if Victimized*,

impacting share and brand value. For example, the Wall Street Journal has noted that companies suffering publicized security breaches in which confidential customer data was compromised experienced a reduction in stock prices.<sup>17</sup>

The Commission, in its *Report and Order*, in adopting the data breach notification requirement, noted that the competitive pressures identified by Charter were not effective if consumers were not aware of breaches.<sup>18</sup> The Commission's statements imply that it agrees with the efficacy of such competitive pressures in driving carriers' privacy and security practices if a notice regime is in place. In fact, the Commission has previously noted that "the carrier with whom the customer has the existing business relationship has a strong incentive not to misuse its customers' CPNI or it will risk losing its customers' business."<sup>19</sup> Now that the Commission has adopted a data breach notification regime, the market incentive for carriers to protect CNPI has intensified and augments the Commission's far-reaching regulatory regime.

Today, the market for telecommunications services is intense. Carriers compete not just on the price and quality of services to which the consumer subscribes, but also on other aspects of a business's practices that customers may value. In such an environment, enhanced privacy

---

ECommerceTimes, Nov. 18, 2005, at <http://www.ecommercetimes.com/story/47422.html> (reporting that a recent survey commissioned by Sun Microsystems indicates that 50 percent of consumers would take their online business elsewhere if they were victims of identity theft at a particular financial institution).

<sup>17</sup> Michael Rappaport, *Companies Pay a Price for Security Breaches*, WALL STREET J., at C3, June 15, 2005.

<sup>18</sup> *Report and Order* ¶ 30, n.98.

<sup>19</sup> *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Third Report and Order and Third Further Notice of Proposed Rulemaking, CC Docket 96-115, 96-149, 00-257, FCC 02-214, ¶ 37 (rel. July 25, 2002) ("*Third Report and Order*"); see also *id.* ¶ 37 n.109 ("[A]s competition continues to develop, this safeguard will only increase in its usefulness.").

and data security practices can distinguish one competitor from another and therefore result in added customers and revenue. If the marketplace, i.e., consumers, demands protection of CPNI and other personal information, innovative carriers will deliver in ways that make sense for their unique business circumstances. This will occur without over-burdensome government mandates. Such competition, while not new, is becoming increasingly robust as privacy and data security issues gain a higher profile in our society.

Recent changes in business privacy practices illustrate how market forces enhance consumer privacy. For example, only recently after Google announced changes limiting data retention policies, other search engines such as Microsoft, Ask.com and Yahoo followed in quick succession with corresponding or even more extensive limitations on their data retention policies.<sup>20</sup> Competitive responses to Google's actions were purely market-driven, occurring despite the lack of any law or regulation requiring them. Such competition in privacy practices has existed for a long time. As Elissa Cooper, policy analyst at the Center for Democracy and Technology recently acknowledged, albeit belatedly, "we're starting to see true competition for privacy. It's a great development that privacy is a point of competition."<sup>21</sup> The market for privacy competition, when combined with the already extremely far-reaching current and supplemented CPNI rules, renders further rules wholly unnecessary.

---

<sup>20</sup> Robert Koman, *Search Engines Compete for Privacy Bragging Rights*, Yahoo News, July 24, 2007.

<sup>21</sup> *Id.*

### **III. THE CONSUMER COALITION'S ARGUMENTS IN SUPPORT OF THE ISSUES RAISED IN THE NPRM ARE NOT PERSUASIVE**

#### **A. Mandating Password Protection for Non-Call Detail CPNI Would be Ill-Advised**

The Commission's stated purpose in adopting a new password requirement for consumer access to call-detail CPNI was to accommodate concerns about customer privacy while enabling carriers to provide "timely customer service."<sup>22</sup> In excluding non-call detail CPNI from the password requirement, the Commission proclaimed its rules "no more extensive than necessary to protect consumers' privacy."<sup>23</sup> Adding a password requirement for release of non-call detail CPNI would make the rules overbroad. Although the Commission considers all CPNI to be "sensitive," such a new requirement would be overbroad because the record the Commission has amassed reflects that pretexters specifically target call-detail CPNI.<sup>24</sup> Without a record showing such information is targeted, the Commission risks violating the First Amendment<sup>25</sup> and the Administrative Procedures Act by expanding the password requirements to non-call detail CPNI.<sup>26</sup> Moreover, carriers still have to authenticate customers making non-call detail inquiries so the information is protected.<sup>27</sup>

---

<sup>22</sup> *Report and Order* ¶ 18.

<sup>23</sup> *Id.* See also *id.* ¶13 n.46 ("By limiting our rules to the disclosure of call detail information, we believe that we have narrowly tailored our requirements to address the problems of pretexting.").

<sup>24</sup> *Id.* at ¶ 14.

<sup>25</sup> See Verizon Comments, at 10-11 (July 9, 2007).

<sup>26</sup> See, e.g., *Nat'l Fuel Gas Supply Corp. v. FERC*, 458 F.3d 831 843 (D.C. Cir. 2006) (vacating a federal agency's order as "not reasoned decisionmaking" and unlawful under the Administrative Procedures Act where the agency "[p]rofessed that an order ameliorate[d] a real industry problem but then cite[d] no evidence demonstrating that there is in fact an industry problem."). See also Sprint-Nextel Corporation Comments, at 6-7 (July 9, 2007).

<sup>27</sup> *Report and Order* ¶ 13.

In addition to being overbroad and unnecessary, a rule expanding the password requirement to non-call detail CPNI is an unwise anti-consumer interference in a carrier's ability to provide service to its customers. As Charter explained in its initial comments, passwords are an annoyance to customers.<sup>28</sup> Charter cited a 2006 Ponemon Institute study indicating that a majority of consumers would prefer not to use a unique password and that 87% of consumers opposed legislatively mandated password requirements.<sup>29</sup> In addition to being disruptive to consumers generally, the record also reflects that passwords for virtually any routine inquiry are particularly disruptive and upsetting to the elderly, handicapped, and non-English speakers.<sup>30</sup>

The Consumer Coalition's argument that a password requirement for both call detail and non-call detail CPNI would "simplif[y] the burden for carriers" is a red herring.<sup>31</sup> Carriers are uniquely suited to assess the efficiency of their own business methods including the training and oversight or investigation of their customer service representatives. If a particular carrier believes it is more efficient to have a uniform standard operating procedure requiring a password for all CPNI-related inquiries, then there is nothing to prohibit a carrier from adopting that approach on its own.

It is particularly ironic that the Commission would consider subjecting Charter and other carriers that are also cable operators to additional requirements that disrupt the ability to provide timely and useful customer service given the Commission's longstanding cable television customer service rules. Under Part 76 of the Commission's rules, cable operators are generally required to answer telephone calls within 30 seconds of the connection and to transfer telephone

---

<sup>28</sup> Charter NPRM Comments, at 25-28.

<sup>29</sup> Charter NPRM Comments, at 25-26. *See also Report and Order* ¶ 13, n.47.

<sup>30</sup> *See National Cable & Telecommunications Association Comments*, at 3 (July 9, 2007) (citing letters and comments in the record).

<sup>31</sup> Consumer Coalition Comments, at 7 (July 9, 2007).

calls within 30 seconds.<sup>32</sup> In addition, the rules specify that callers should not receive busy signals more than 3% of the time.<sup>33</sup>

Expanded password requirements will undoubtedly result in Charter customer service representatives (“CSRs”) spending more time with each caller as they explain why they cannot readily provide, without a password, basic non-call detail information, such as the minutes remaining on a call-plan, the balance due on an account, the customer’s rate plan or the date and amount of the last payment. With the CSRs dedicated to voice customers tied-up for longer periods of time, Charter’s ability to timely respond to all customers will be harmed, jeopardizing not just customer relations generally, but also its ability to comply with the cable customer service rules. This puts cable operators like Charter at risk of enforcement action not just by the Commission, but also by individual local franchising authorities throughout the country who have the authority to enforce the cable customer service rules.<sup>34</sup>

#### **B. The Costs of Audit Trails Outweigh the Consumer Benefits**

In the *FNPRM*, the Commission cited Charter’s initial *NPRM* comments concerning the expense of audit trails in comparison to the consumer benefits.<sup>35</sup> As Charter previously pointed out, the Commission adopted an audit trail mandate in 1998, but after reconsideration, it promptly eliminated the requirement in 1999. Prompting the Commission’s reconsideration were reports from numerous carriers citing costs in the millions of dollars to implement the audit trail requirement, ranging from Sprint’s estimate of \$19.6 million to AT&T’s estimate of \$270

---

<sup>32</sup> See 47 C.F.R. § 76.309(c)(ii).

<sup>33</sup> *Id.* at § 76.309(c)(iv).

<sup>34</sup> *Id.* at § 76.309(a).

<sup>35</sup> *FNPRM* ¶ 70.

million.<sup>36</sup> In 1999, when the Commission weighed the costs and benefits, it found that “on balance, such a potentially costly and burdensome rule does not justify its benefit.”<sup>37</sup> As discussed by numerous commenters to the *FNPRM*, that rationale for not extending the audit trail requirement holds true today.<sup>38</sup>

Like other carriers, Charter is not aware of any technological developments since the *Report and Order* that would significantly reduce the cost of an audit trail requirement. As a relatively new entrant to large-scale voice services operations, Charter in many instances relies on its existing cable television customer management infrastructure.<sup>39</sup> The costs of compliance with a new audit requirement for Charter remain large. Notably, the Consumer Coalition provides no information demonstrating the costs of a comprehensive audit trail system are small, even for carriers that already track customer service inquiries for certain internal business purposes.

Moreover, any consumer benefits from audit trails would be minimal and not justified by the costs. As the Commission itself noted, the “record indicates 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 consumer inquiry.”<sup>40</sup> Also, even if an

---

<sup>36</sup> *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, Order on Reconsideration and Petitions for Forbearance*, 14 F.C.C.R. 14409, ¶ 124 (Aug. 16, 1999 (hereinafter *Reconsideration Order*)).

<sup>37</sup> *Id.* at ¶ 127.

<sup>38</sup> *See, e.g.*, Time Warner Comments, at 9 (July 9, 2007); Verizon Comments, at 13 (July 9, 2007); Comcast Comments at 7 (July 9, 2007); T-Mobile USA, Inc. Comments, at 5 (July 9, 2007).

<sup>39</sup> *See* Sprint Nextel Corporation Comments, at 12 (July 9, 2007) (explaining the technical difficulties different operating systems and applications pose, which make it costly to implement audit trails).

<sup>40</sup> *FNPRM* ¶ 69.

instance of improper CPNI disclosure occurs because of pretexting, the audit trail would likely be of very little help in locating a pretexter, since the trail would only reflect that someone claiming to be a customer sought the information.<sup>41</sup> For these reasons, Charter remains opposed to any new audit trail requirements.

### **C. Specific Mandates for Physical Safeguards are Unnecessary**

As discussed above, Section 222 of the Communications Act already imposes a duty on carriers to protect CPNI. To the extent there were any doubts about the Commission's ability to enforce that requirement, the Commission, in its *Report and Order* eliminated them by codifying that duty in its rules.<sup>42</sup> In imposing this requirement, yet not mandating specific technological measures to protect CPNI, the Commission took a reasoned practical approach that accounts for differences in carriers' operations and allows them to weigh the individual benefits and costs of different security practices. Certainly, what may be practical for one carrier, may not be for another. However, this approach clearly does not mean the Commission allows carriers to *avoid* implementing reasonable protective measures. In its *Report and Order*, the Commission emphasized carriers' responsibility to remain vigilant and "stress[ed its] expectation that carriers will take affirmative measures to discover and protect against . . . [pretexting] beyond what is required by the Commission's current rules."<sup>43</sup>

The Consumer Coalition advocates for mandatory encryption of stored CPNI, minimization of carrier employee access to CPNI, and audit trails to track employee access to CPNI. Once again, the Consumer Coalition, in advocating for as broad a regulatory regime as possible, does not acknowledge crucial factors such as the costs to carriers to implement changes

---

<sup>41</sup> See AT&T Comments, at 8 (July 9, 2007).

<sup>42</sup> See *Report and Order*, Appendix B (listing the addition of 47 C.F.R. § 64.2010(a)).

<sup>43</sup> *Report and Order* ¶ 35.

(particularly when weighed against the risks), the market incentive to protect CPNI, the efficacy of enforcing criminal laws against pretexting, or the statutory and soon regulatory requirement that exists and which requires carriers to protect CPNI. The mandatory encryption proposal illustrates the problem with ignoring these factors.

As Charter explained in its initial NPRM comments, the costs to implement and maintain a system of mandatory encryption can be very high.<sup>44</sup> Because of the substantial cost, “a company’s decision to encrypt its data, and the type of encryption technology to employ, is highly dependant on whether the benefits of encrypting data outweigh not only the financial expenditures, but the costs associated with decreases in performance and data access speed.”<sup>45</sup> The costs of encryption must also be considered with the record evidence showing that CPNI stored in carrier databases has not been targeted by hackers and the vulnerabilities that even encrypted data presents.<sup>46</sup> In fact, many of the comments in the *FNPRM* similarly note the significant expense involved with encryption and the lack of corresponding guarantee in security.<sup>47</sup>

The Consumer Coalition also fails to make a compelling case for new rules requiring audit trails of employee access and minimization of employee access. For the same reasons addressed above in Part II.B, an employee audit trail would be prohibitively expensive. And Charter already restricts access to CPNI to those employees with a need to access and use the

---

<sup>44</sup> See Charter NPRM Comments, at 29 (citing Alison Diana, *Benchmarking Encryption Technology*, ECOMMERCE TIMES, Aug. 12, 2003, <http://www.ecommercetimes.com/story/31311.html>).

<sup>45</sup> *Id.*

<sup>46</sup> *Report and Order* ¶ 36.

<sup>47</sup> See, e.g., Verizon Comments, at 16 (July 9, 2007) (“A requirement to encrypt records would impose significant costs that cannot be justified, particularly in the absence of any demonstrated benefit in deterring data brokers or enhancing security beyond its current level.”).

information for customer service and operational support. However, carriers like Charter, because of the number of subscribers and geographic scope of services provided, must have to have a fairly significant number of customer relations employees with access to CPNI to provide effective customer service. Specific rules undoubtedly would, for some companies, unduly limit the number of employees with access to CPNI in a manner that hampers efficient operations.

The Commission's "reasonableness" standard already requires that carriers adopt safeguards appropriate to their circumstances, which might include some of the specific steps proposed by the Commission or even others that have not been discussed. As Charter explained in its initial NPRM comments, a "reasonableness" standard provides the Commission and carriers with greater flexibility to adopt effective security practices:

Because reasonableness is measured by current norms and practices, the Commission can more rapidly adjust its policies to respond to changes in the industry and react to evolving threats. Such an approach is more responsive than imposing specific mandates, especially in a situation like that with CPNI, where it is inherently difficult for an agency to mandate specific practices without the danger that those practices will become obsolete, requiring ever more rule revisions and rulemakings.<sup>48</sup>

#### **D. Limiting Data Retention Would Be Complex and Unworkable**

The Consumer Coalition does not provide compelling reasons to implement a deletion or de-identification requirement for CPNI records, especially in light of record evidence demonstrating that recent, not historical CPNI is usually what is targeted by pretexters.<sup>49</sup> The record also reflects various reasons carriers may need to retain data. In addition to billing disputes and contractual requirements, which Charter identified in its initial NPRM comments,<sup>50</sup>

---

<sup>48</sup> Charter NPRM comments at 24.

<sup>49</sup> *See, e.g.*, Time Warner Comments, at 11 (July 9, 2007); AT&T Comments, at 8 (July 9, 2007).

<sup>50</sup> Charter NPRM Comments, at 30.

Charter agrees with the many other commenters who note that mandatory data retention requirements might conflict with various record retention regulations. For example, both Comcast and Verizon identify various rules and business reasons for maintaining CPNI.<sup>51</sup> In addition, as the Commission notes, the Department of Justice has been advocating longer, not shorter retention periods.<sup>52</sup>

A de-identification approach as an alternative to early deletion is also unworkable. As Charter explained in its initial comments, a de-identification approach would be particularly costly and time-consuming.<sup>53</sup> Deleting entire records merely requires a carrier to identify CPNI that is older than a preset date and then delete it. To de-identify a record, the carrier must implement a more complex program that first identifies which CPNI is older than some preset date (unless all CPNI must immediately be de-identified) and then isolates the “data that identify a particular caller from the general transaction records.”<sup>54</sup> Presumably, identifiable data would include the customer’s name, address, and account number, as well as the customer’s phone number. Thus, identifying such data requires a complex algorithm for parsing the record and removing every instance where identifiable data appears. This complex solution would be prohibitively expensive to implement, and would burden a carrier’s system by requiring it to monitor and edit CPNI records for each and every consumer on a daily basis. And if only applied to older records, modifying such records would have no effect on the availability of more recent CPNI, which as explained above, appears to be most vulnerable to unauthorized

---

<sup>51</sup> See Comcast Comments at 8-9; Verizon Comments at 18-19.

<sup>52</sup> *FNPRM* ¶ 71. See also Charter NPRM Comments at 31; Charter NPRM Reply Comments at 18 (June 2, 2006).

<sup>53</sup> Charter NPRM Comments, at 31.

<sup>54</sup> *CPNI NPRM* ¶ 20.

disclosure. Even more significant would be the costs and administrative complexity of re-identifying records as necessary to respond to consumer or government requests.

For all of these reasons, the Commission should adhere to the position it took in the *Reconsideration Order* where it concluded that carriers should have “the flexibility to adapt their record keeping systems in a manner most conducive to their individual size, capital resources, culture and technological capabilities.”<sup>55</sup>

#### **IV. THE CONSUMER COALITION’S “ADDITIONAL RECOMMENDATIONS” ARE ILL-ADVISED**

In addition to addressing the issues raised in the *FNPRM*, the Consumer Coalition also advocates for additional rules the Commission has not even mentioned. In particular, the Consumer Coalition argues for rescinding the law enforcement delay provision for customer notice of unauthorized access to CPNI and urges the Commission to make customer “opt-in” the rule for all CPNI sharing. Again, the Consumer Coalition ignores the comprehensive nature of the recently supplemented rules, the costs of the proposals, the efficacy of enforcing laws that criminalize pretexting, and the effects of competition. Both proposals are unnecessary and contrary to the public interest.

##### **A. Eliminating the Law Enforcement Delay Provision Could Harm Investigations**

The Consumer Coalition argues against a law enforcement delay provision for customer notices of unauthorized acquisition of CPNI while giving virtually no regard for the needs of law enforcement. Disclosure of a breach can jeopardize a criminal investigation and once a notice is sent to a consumer, neither a carrier nor law enforcement can control its further dissemination. It is therefore with good reason that virtually every data breach notification regime addressing

---

<sup>55</sup> *Reconsideration Order* ¶ 7(f).

personally identifiable information, which encompasses Gramm-Leach-Bliley Act regulations and data breach notification laws applicable to businesses in thirty-eight states plus Washington, D.C. and Puerto Rico, has a law enforcement delay provision.<sup>56</sup>

The Consumer Coalition would only support a law enforcement delay exception in the “rare event” that notification might compromise national security and, even then, only if disclosure might result in immediate and irreparable harm.<sup>57</sup> Under the Consumer Coalition’s proposal, any such delay could last only 7 days. The Consumer Coalition fails to recognize the importance of catching criminals both to deter crime and to recover or prevent misuse of data obtained in an instance of pretexting or data theft.<sup>58</sup> This is particularly true where a breach incident may involve unauthorized access to numerous customers of a carrier, rather than a single, isolated individual. Moreover, the Commission has already addressed the Consumer Coalition’s concerns about harms from domestic violence by including a mechanism for immediate notice in consultation with law enforcement based on urgent need.<sup>59</sup>

**B. Requiring Opt-In for All Sharing of CPNI is Bad Policy and Violates the First Amendment**

The CPNI rules, as supplemented by the *Report and Order* are already extremely restrictive when it comes to a carrier’s ability to share CPNI. Customer approval is required for all sharing by a carrier of CPNI for marketing purposes, even if the CPNI is provided to

---

<sup>56</sup> See, e.g., Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (codified at 12 C.F.R. pt. 30, app. B, Supplement A; 12 C.F.R. pt. 208, app. D-2, Supplement A; 12 C.F.R. pt. 225, app. F, Supplement A; 12 C.F.R. pt. 364, app. B, Supplement A; 12 C.F.R. pt. 570, app. B, Supplement A); CAL. CIV. CODE § 1798.82(c) (2006). The California law has served as the model upon which subsequent state data breach notification laws have been based.

<sup>57</sup> Consumer Coalition Comments, at 21.

<sup>58</sup> *Report and Order* ¶ 28.

<sup>59</sup> *Id.*

affiliates. The sole exception is when CPNI is shared with an affiliate who already serves the same customer with a communications-related service, which, notwithstanding the age of convergence, does not include all of the services offered by a broadband provider.<sup>60</sup> And soon, with the recent rule amendments, customer approval must be opt-in for a carrier to share CPNI for marketing purposes with unaffiliated third parties, with affiliates if to market non-communications-related services, *and* with joint venture partners or independent contractors even if to market communications-related services. The Consumer Coalition wants the Commission to go even further and extend an opt-in mandate to sharing with a carrier's affiliates and its agents for marketing communications-related services or for any use by a carrier of CPNI for marketing purposes (even without sharing).<sup>61</sup>

Extending the opt-in requirements even further is not needed to protect consumers and would violate the First Amendment. The Consumer Coalition presents two major related arguments as to why there should be a comprehensive opt-in regime. They argue opt-out “is not calculated to reasonably inform consumers about their privacy options” and it increases transaction costs for consumers because there is “an economic incentive for businesses to make it difficult for consumers to exercise their preference not to disclose personal information to others.”<sup>62</sup> The primary problem with the Consumer Coalition's arguments is that they are made without any regard to the other existing CPNI rules.

As Charter explained in its initial comments, the Commission has designed the CPNI rules to provide an adequate opportunity for consumers to be informed of, and to exercise, their privacy choices at all times, by implementing numerous “choice safeguards” to preserve the

---

<sup>60</sup> See 47 C.F.R. §§ 64.2005(a); 64.2003(b)(3).

<sup>61</sup> Consumer Coalition Comments, at 22.

<sup>62</sup> *Id.* at 22-23.

customer's ultimate control over their CPNI.<sup>63</sup> These significant safeguards alleviate any concerns about notices not being designed to inform customers of their options or carriers acting to purposefully increase consumer transaction costs involved in exercising opt-out choice. For example, under the current CPNI rules, carriers must give customers adequate notice and opportunity to opt-out every two years,<sup>64</sup> with the rules specifying in detail the content of such notification.<sup>65</sup> Among other things, the notices must "be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer."<sup>66</sup> In addition, after mailing notices, the carrier must then wait at least 30 days before assuming that the customer has consented, i.e., decided not to opt-out pursuant to the notice.<sup>67</sup> Even after a carrier has obtained the customer's opt-out approval, the carrier must additionally provide the opportunity to opt-out at no cost to the customer, 24 hours a day, seven days a week.<sup>68</sup> A customer's ability to exercise choice and to stay informed of their options under the current rule regime counsels against a broader opt-in approach.

The Consumer Coalition also ignores the effects of competition, as discussed in Part II.B above, on the quality of information provided to consumers and the ease with which a consumer can exercise opt-out choice. For example, Charter not only mails customers CPNI notices every

---

<sup>63</sup> Charter NPRM Comments, at 18; Charter NPRM Reply Comments, at 6.

<sup>64</sup> 47 C.F.R. § 64.2008(d)(2).

<sup>65</sup> 47 C.F.R. § 64.2008(c).

<sup>66</sup> *Id.*

<sup>67</sup> 47 C.F.R. § 64.2008(d)(1).

<sup>68</sup> *See Third Report and Order* ¶ 118 (allowing carriers the freedom to select the method for providing an opt-out mechanism, "so long as all customers are able to access and use those mechanisms, 24 hours a day, seven days a week"). The Commission suggested that such mechanisms may include "a postage-paid return postcard, a toll free number, a secure Internet page, and/or an email address to receive opt-outs." *Id. But cf.* 47 C.F.R. § 64.2008(d)(3)(v) (requiring a 24-hour, seven days a week, opt-out mechanism for telecommunications carriers that use e-mail to provide opt-out notices).

two years, it keeps its CPNI notice posted on its web site consistent with industry practice. If it becomes widely known that a company will not honor its customers' opt-in choices or it makes it difficult to exercise such choice, that company will likely be punished in the marketplace.

A total opt-in regime also would violate the First Amendment. While Charter does not necessarily agree with the Commission's analysis, its extensive discussion in the *Report and Order* as to why its changes to the opt-in rules did not violate the First Amendment focused on a carrier's sharing of CPNI with independent contractors and joint venture partners, not with affiliates and agents. The Commission will have a serious problem meeting the narrow tailoring prong of the First Amendment's commercial speech jurisprudence if it goes as far as the Consumer Coalition is pushing.

## **V. CONCLUSION**

For the reasons set forth above, the Commission should not adopt any of the items discussed in the *FNPRM* or the other proposals advanced by the Consumer Coalition. Commenters and Charter have demonstrated that new rules are unnecessary and would impose significant costs on carriers without any appreciable benefits to consumers. The CPNI rules as supplemented in the *Report and Order* are very extensive and far-reaching. And apart from the rules, carriers already have adequate incentives to protect CPNI. Those that do not do so will lose existing customers or find themselves unable to acquire new ones.

