

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

In the Matter of	)	
	)	
Implementation of the Telecommunications Act	)	CC Docket No. 96-115
of 1996:	)	
	)	
Telecommunications Carriers' Use of Customer	)	
Proprietary Network Information and Other	)	
Customer Information;	)	
	)	
IP- Enabled Services	)	WC Docket No. 04-36
	)	
	)	
_____	)	

**REPLY COMMENTS OF VERIZON**

Michael E. Glover  
Of Counsel

Karen Zacharia  
Mark J. Montano  
VERIZON  
1515 N. Court House Road  
Suite 500  
Arlington, VA 22201-2909

Dated: August 7, 2007

Counsel for Verizon

## TABLE OF CONTENTS

	<b>Page</b>
I. THE BURDENS OF PASSWORD REQUIREMENTS FOR ALL CPNI AND THEIR LIMITED BENEFITS ARE WELL-RECOGNIZED.....	2
II. THERE IS NO EVIDENCE THAT ADDITIONAL PROTECTIVE MEASURES WOULD JUSTIFY THEIR STEEP COSTS. ....	6
A. Preparing Audit Trails of All CPNI Disclosures Continues To Be Unduly Burdensome. ....	6
B. Requiring Particular Physical Safeguards, Such as Encryption, Is Unnecessary To Protect CPNI. ....	8
C. Carriers Require Flexibility in Their Data Retention Practices To Meet a Variety of Objectives and Legal Requirements, Including Protection of CPNI. ....	10
III. COMPREHENSIVE OPT-IN REQUIREMENTS ARE UNECESSARY AND WOULD VIOLATE THE FIRST AMENDMENT.....	11
IV. CONCLUSION.....	16

**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 VERIZON**

Nearly all commenters agree that the Commission should exercise restraint in its approach as it considers whether any modifications to its recently pronounced CPNI rules<sup>1</sup> may be appropriate, particularly when public attention has caused data brokers<sup>2</sup> and pretexters to now face federal and state criminal exposure, private lawsuits, and increased carrier security measures. The effectiveness of the Commission's new CPNI rules, which have yet to be implemented, requires a thorough evaluation before the Commission could conclude that additional, burdensome CPNI safeguards would be necessary.

Although EPIC submitted comments (as part of the "Consumer Coalition") renewing its support for additional regulations pertaining to passwords, audit trails, physical safeguards, and data deletion, it failed to provide any evidence that these measures are needed or that the

---

<sup>1</sup> Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) ("2007 CPNI Order").

<sup>2</sup> Verizon uses the term "data brokers" to refer to persons who claim to be able to provide CPNI to others for a fee.

potential increase in security from more stringent requirements outweighs the substantial burdens they would impose on customers and carriers. Similarly, there is no compelling reason for the Commission to re-examine its new rules with respect to opt-in consent.<sup>3</sup>

**I. THE BURDENS OF PASSWORD REQUIREMENTS FOR ALL CPNI AND THEIR LIMITED BENEFITS ARE WELL-RECOGNIZED.**

The Commission's new CPNI rules require a customer to provide a password in order to receive call detail information from a carrier's customer service representative in a customer-initiated call.<sup>4</sup> The Consumer Coalition and the New Jersey Division of Rate Counsel ("NJ Rate Counsel") now argue that the Commission should extend these rules even further so that instead of the standard authentication methods used by the carrier, a customer must provide a password before a carrier can disclose *any* CPNI, including basic account information.<sup>5</sup> This would include disclosure of information like a bill balance, which a customer might require in order to avoid disconnection, or even a listing of existing services on the customer's line, which is often necessary to avoid sales of incompatible products and services. However, as almost all commenters agree, such a requirement would unduly hinder transactions between customers and

---

<sup>3</sup> In addition, the record does not support the Commission's placing further restrictions on the sale of CPNI, which the Consumer Coalition mentions in passing in the introduction to its comments. *See* Comments of Consumer Action *et al.* ("Consumer Coalition") (July 9, 2007) at 1. A broad prohibition on the sale of CPNI to recipients other than a telecommunications provider with whom the customer has a current business relationship as the Consumer Coalition urges could potentially be read to bar a variety of legitimate transactions, including a carrier's cessation of service in a particular region by selling assets to another provider or the sale of debt to a collector.

<sup>4</sup> 2007 CPNI Order ¶ 13.

<sup>5</sup> *See* Comments of Consumer Coalition at 7; Comments of NJ Rate Counsel (July 9, 2007) at 5.

carriers while providing little added privacy protection.<sup>6</sup> Therefore, the Commission should not expand its newly established password requirements.

Although it provides no evidence in support, the Consumer Coalition incredibly claims that expanding the password requirement would in fact *decrease* the burden on customers and carriers.<sup>7</sup> According to the Consumer Coalition, because customers do not understand what CPNI is and how it relates to privacy (and carriers have failed to explain it adequately),<sup>8</sup> they would not know whether or when to provide a password during a call they initiated.<sup>9</sup> Similarly, the Consumer Coalition contends that the password requirement would be “eas[y]” for carriers to implement because customer service representatives would be able to follow the same

---

<sup>6</sup> See, e.g., Comments of Sprint Nextel Corporation (July 9, 2007) at 7 (noting that customers expect ready access to “relatively benign” categories of CPNI, such as minutes of use, rate plan, and balance); Comments of Qwest Communications International Inc. (July 9, 2007) at 5-7; Comments of Comcast Corporation (July 9, 2007) at 4-5 (observing that most customer calls relate to billing); Comments of Time Warner Inc. (July 9, 2007) at 8 (expecting substantial customer frustration if one cannot access “vertical features associated with his current plan or the minutes remaining on a measured-usage plan”); Comments of Frontier Communications (July 9, 2007) at 3-4 (noting that customers would be frustrated if carriers could not respond to inquires regarding charges or adding/subtracting services like Caller ID without a password); Comments of AT&T Inc. (July 9, 2007) at 5; Comments of the Iowa Telecommunications Association (“ITA”) (July 9, 2007) at 3-4; Comments of the National Cable and Telecommunications Association (July 9, 2007) at 3 (asserting that passwords “may be particularly burdensome for certain groups of customers, such as senior citizens, people with disabilities, or non-English speaking customers”).

<sup>7</sup> Comments of Consumer Coalition at 7.

<sup>8</sup> The Consumer Coalition criticizes Verizon’s CPNI notice because it purportedly fails to include the term “privacy” and explicitly state that CPNI includes a person’s calling records. *Id.* n.35. Verizon’s CPNI notice states in part: “[W]e have the duty to protect the confidentiality of your telecommunications service information. This information includes the services and products you purchase, account activity (for example the telephone numbers you dial), and charges incurred.” Verizon’s definition is consistent with the definition of CPNI used by the Commission and certainly encompasses call detail information in the parenthetical. The absence of the term “privacy” is of no consequence since the definition of CPNI in 47 U.S.C. § 222(h)(1) also lacks that term and the notice instead uses a common synonym – “confidentiality.”

<sup>9</sup> Comments of Consumer Coalition at 7.

verification procedure each time a customer called and it would be “simpl[e]” for a carrier to determine employee compliance.<sup>10</sup> Finally, NJ Rate Counsel argues that there would be no higher burdens on customers and carriers from an enhanced password requirement if passwords are already required for some CPNI disclosures.<sup>11</sup>

Contrary to the Consumer Coalition’s claims, carriers understand the difference between call detail and non-call detail CPNI, and customers would not have to make that determination under the Commission’s new rules. As a result, rather than reducing the burden on customers, a password requirement for all CPNI would substantially increase the burden by requiring customers to remember a password in order to obtain basic account information, such as their bill balance or rate plan. The Consumer Coalition and NJ Rate Counsel simply ignore the well-established burdens on customers of recalling passwords and the burdens on carriers of providing their entire customer base with passwords and having to reset them when many are inevitably forgotten. If the Consumer Coalition is correct that customers are seriously challenged by terms like CPNI or cannot comprehend what call detail information is,<sup>12</sup> customers could not be expected to consistently recall their passwords nor understand why a password is necessary for basic account questions and service changes. Moreover, NJ Rate Counsel’s comments fail to consider that requiring passwords for all CPNI disclosures in a customer-initiated call would in practice require all customers to be issued passwords since customer inquiries requiring a customer service representative to disclose call detail information occur much less frequently than calls that involve the disclosure of non-call detail CPNI.

---

<sup>10</sup> *Id.*

<sup>11</sup> Comments of NJ Rate Counsel at 5.

<sup>12</sup> Comments of Consumer Coalition at 7.

As with its analysis of the burdens, the Consumer Coalition mischaracterizes the benefits of password protection. The Consumer Coalition asserts that failing to require a password for all CPNI would “only open[] a loophole for pretexters to exploit.”<sup>13</sup> However, the Consumer Coalition does not – and cannot – provide any evidence that pretexters and data brokers have sought or value non-call detail CPNI. Verizon and other commenters are aware of nothing to suggest that non-call detail CPNI has been systematically targeted by pretexters even though passwords are not required today.<sup>14</sup> Therefore, closing this supposed “loophole” would be unlikely to provide any privacy benefits.

NJ Rate Counsel cryptically argues that the “issues are much broader than the publicized issue of pretexting,” but then fails to explain what those issues may be in relation to a password requirement.<sup>15</sup> NJ Rate Counsel’s observation that “there is no empirical data that customers make distinctions between call and non-call detail”<sup>16</sup> misses the point. Data brokers and pretexters do make those distinctions, which is why the Commission concluded in its *2007 CPNI Order* that only call detail information “presents an immediate risk to privacy.”<sup>17</sup>

In sum, the vast majority of commenters approve of the Commission’s balancing approach in its *2007 CPNI Order* and believe that the costs of extending the password requirement to include all disclosures of CPNI in customer-initiated calls would outweigh any

---

<sup>13</sup> *Id.*

<sup>14</sup> See Comments of Verizon (July 9, 2007) at 9; see also Comments of Sprint Nextel at 8 (“[T]here is no record of CPNI abuse of this type information.”); Comments of Qwest at 7 (“[D]oes a fraudster care if a customer has a ‘do not solicit’ service, or used call waiting 3 times in the past month for a total charge of \$2.25?”); Comments of T-Mobile USA, Inc. (July 9, 2007) at 4; Comments of Comcast at 5.

<sup>15</sup> Comments of NJ Rate Counsel at 5.

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

<sup>17</sup> *2007 CPNI Order* ¶ 13.

benefits. No evidence exists that the Commission's balancing was in error then or would be so today.

**II. THERE IS NO EVIDENCE THAT ADDITIONAL PROTECTIVE MEASURES WOULD JUSTIFY THEIR STEEP COSTS.**

**A. Preparing Audit Trails of All CPNI Disclosures Continues To Be Unduly Burdensome.**

The benefits and burdens of audit trails have been debated for almost ten years. The Commission has twice rejected audit trails because they are not closely targeted to protecting CPNI and are inordinately expensive.<sup>18</sup> Nearly all commenters agree that the Commission's rationale still holds.<sup>19</sup>

The Consumer Coalition stands alone in opposition, arguing that audit trails would help track improper access by a carrier's employees and prosecuting (and thus deterring) pretexters.<sup>20</sup> The Consumer Coalition asserts that audit trails would cause only a limited burden on carriers, which tend to track customer service inquiries and thus already "own the infrastructure required to record all attempts to access a customer's record."<sup>21</sup> However, the Consumer Coalition's assessment of the benefits and the burdens of audit trails cannot withstand scrutiny.

There are numerous other equally capable, but less costly processes in place today to track improper employee access. As Verizon noted in its comments, Verizon's call center systems and databases employ access controls, which allow only authorized personnel to access

---

<sup>18</sup> See *id.* ¶ 64.

<sup>19</sup> See, e.g., Comments of Verizon at 11-15; Comments of Sprint Nextel at 11-12; Comments of Qwest at 9-10; Comments of T-Mobile at 5; Comments of Time Warner at 9-10.

<sup>20</sup> Comments of Consumer Coalition at 8-9.

<sup>21</sup> *Id.* at 9.

these systems and only in appropriate circumstances.<sup>22</sup> Moreover, Verizon has implemented tools to prevent improper access attempts and assist in the detection of a pattern of improper access attempts, whether by employees or outsiders, in both the call center and online settings.<sup>23</sup> Other carriers have similar systems in place.<sup>24</sup> There is no evidence that audit trails would be superior to these existing safeguards since audit trails would only show that employees accessed CPNI, not that employees improperly disclosed it.

In addition, the Consumer Coalition fails to explain how adopting audit trail requirements would address the data broker problem.<sup>25</sup> It appears that in most cases, data brokers obtain confidential customer data by pretending to be someone who can legitimately access customer data. If pretexting is the data brokers' primary means of obtaining customer data (and there is no reason to believe otherwise), then an audit trail may reveal only that someone purporting to be the customer called and asked about customer detail – something that would not be helpful in preventing data broker access to such records or tracking the wrongdoer to a specific person.

Finally, the Consumer Coalition's assertion that carriers have the infrastructure for audit trails already in place because they log certain customer inquiries is factually incorrect. Verizon and other carriers necessarily track certain customer service inquiries and account changes in order to run their businesses, but that does not mean that carriers would be able to record every

---

<sup>22</sup> Comments of Verizon at 17.

<sup>23</sup> *Id.* at 14.

<sup>24</sup> *See, e.g.*, Comments of Sprint Nextel at 10; Comments of Qwest at 8; Comments of T-Mobile at 5; Comments of Comcast at 2-3; Comments of AT&T Inc. at 7; Comments of Rural Cellular Association (July 9, 2007) at 6.

<sup>25</sup> Indeed, audit trails may even compromise federal law enforcement investigations by tipping off a target. *See* Joint Comments of NuVox Communications and XO Communications, LLC (July 9, 2007) at 6 (citing Reply Comments of the U.S. Department of Justice and the Federal Bureau of Investigation (Nov. 19, 2002) at 16).

item of CPNI that is disclosed. Commenters indicate that extensive software upgrades would be required to track all CPNI disclosures.<sup>26</sup> More importantly, the recordation of certain customer service inquiries is not a new phenomenon that post-dates the Commission’s prior analysis of the costs of audit trails on carriers.<sup>27</sup> The Consumer Coalition provides no reason to conclude that the Commission’s reliance on prior carrier estimates to comply with audit trail requirements – including one that exceeded \$270 million – no longer holds.<sup>28</sup> As a result, an audit trail requirement continues to be “a potentially costly and burdensome rule [that] does not justify its benefit.”<sup>29</sup>

**B. Requiring Particular Physical Safeguards, Such as Encryption, Is Unnecessary To Protect CPNI.**

The Commission concluded in its *2007 CPNI Order* that it was unnecessary to require encryption of CPNI given carriers’ general duty to protect CPNI.<sup>30</sup> Most commenters agree that the Commission should not require carriers to encrypt their records as this would impose significant costs that cannot be justified, particularly in the absence of any demonstrated benefit in enhancing security beyond its current level or deterring data brokers, who proceed by deceit

---

<sup>26</sup> See Comments of ITA at 4-5 (“While many billing providers have the capability to track certain account access and service order activity, extensive software upgrades would be required in order to properly detect and log all access to CPNI.”); Comments of the ICORE Companies (July 9, 2007) at 4 (“While small ILECs necessarily record customer account changes, very few have the systems’ capacity or capability to create the kind of extensive audit trail contemplated in the Further Notice. The cost of the required software changes would be prohibitive for most small companies.”).

<sup>27</sup> See Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409 ¶ 126 (1999) (“*Reconsideration Order*”).

<sup>28</sup> *Id.* ¶ 123; see also Comments of the United States Telecom Association (July 9, 2007) at 4-5 (citing substantial cost estimates by carriers that the Commission referred to in its *Reconsideration Order*). In fact, commenter Comcast predicts that the costs for an audit trail would be even higher today. Comments of Comcast at 7.

<sup>29</sup> *Reconsideration Order* ¶ 126.

<sup>30</sup> *2007 CPNI Order* ¶ 36.

and impersonation, rather than hacking.<sup>31</sup>

The Consumer Coalition again argues otherwise. It considers the substantial cost of encryption to be irrelevant in the context of sensitive customer data.<sup>32</sup> If costs are considered, the Consumer Coalition suggests that carriers can reduce their encryption costs by retaining less CPNI.<sup>33</sup>

Contrary to the Consumer Coalition’s claims, the costs of encryption do matter. In its *2007 CPNI Order*, the Commission stated, “[A]lthough we do not specifically require carriers to encrypt their customers’ CPNI, we expect a carrier to encrypt its CPNI databases if doing so would provide significant additional protection against the unauthorized access to CPNI *at a cost that is reasonable given the technology a carrier already has implemented.*”<sup>34</sup> Thus, the costs of supplemental encryption – which Verizon estimates to be tens of millions of dollars – are critical to the determination of whether a carrier’s protection of CPNI is reasonable.

Finally, the Consumer Coalition’s claim that encryption costs would be lower if there were less data to encrypt merely states the obvious. While total encryption costs may be slightly lower, that cost savings would not be sufficient to cause the encryption of all CPNI to be feasible. What’s more, less data to encrypt would only lower a carrier’s initial encryption costs because carriers would still need to encrypt every new CPNI datum that is created. As discussed

---

<sup>31</sup> See, e.g., Comments of Sprint Nextel at 14-15; Comments of T-Mobile at 6; Comments of Comcast at 8.

<sup>32</sup> Comments of Consumer Coalition at 10.

<sup>33</sup> *Id.*

<sup>34</sup> *2007 CPNI Order* ¶ 64 (emphasis added); see also *Reconsideration Order* ¶ 5 (stating that the Commission’s goal is “to carry out vigilantly Congress’ consumer protection and privacy aims, while simultaneously reducing the burden of carrier compliance with section 222 by eliminating unnecessary expense and administrative oversight”).

below,<sup>35</sup> carriers retain data for a variety of legitimate reasons, including their obligation under 47 U.S.C. § 222(c)(2) to disclose it upon customer request, and cannot simply discard data to lower the cost of encryption, particularly when the Consumer Coalition provides no evidence of a relationship between encryption and pretexting.<sup>36</sup>

**C. Carriers Require Flexibility in Their Data Retention Practices To Meet a Variety of Objectives and Legal Requirements, Including Protection of CPNI.**

While all commenters but the Consumer Coalition agree that it is not necessary for the Commission to limit data retention to protect CPNI from data brokers,<sup>37</sup> the Consumer Coalition reprises EPIC’s arguments from 2005 that data should be deleted when it is no longer needed for billing purposes or disputes because the deletion of CPNI “is the most secure and certain way to eliminate risk.”<sup>38</sup> However, the Consumer Coalition fails to provide any evidence of a risk to older records, particularly when the Commission “strengthen[s] [its] privacy rules” that “will sharply limit pretexters’ ability to obtain unauthorized access”<sup>39</sup> to CPNI and Congress and many states have recently criminalized pretexting.<sup>40</sup> Nor does the Consumer Coalition address the numerous existing regulations that address data retention and may conflict with its proposal,

---

<sup>35</sup> See *infra* § II.C.

<sup>36</sup> The Consumer Coalition also asserts that employee access to CPNI should be limited and audit trails should be employed to track employee access. As discussed *supra*, Verizon already limits access to CPNI and has reasonable safeguards in place to combat the risk of employee intentional misconduct.

<sup>37</sup> See, e.g., Comments of Sprint Nextel at 15-16 (noting that data brokers highly value CPNI that is most recent and available through low-tech means); Comments of Qwest at 13; Comments of T-Mobile at 7; Comments of Time Warner at 11; Comments of AT&T Inc. at 8 (observing that “dated information has minimal, if any, benefit to pretexters”); Comments of ITA at 6.

<sup>38</sup> Comments of Consumer Coalition at 14.

<sup>39</sup> 2007 CPNI Order ¶¶ 1-2.

<sup>40</sup> See, e.g., Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039.

including the Commission's Part 42 rules,<sup>41</sup> state regulations,<sup>42</sup> and the Fair Credit Reporting Act.<sup>43</sup>

The Consumer Coalition similarly fails to dispute the legitimate business and law enforcement needs set forth by commenters for retaining CPNI data for certain lengths of time, except with respect to carriers' marketing.<sup>44</sup> Contrary to the Consumer Coalition's suggestion,<sup>45</sup> marketing is also a legitimate business purpose, which enjoys First Amendment protection. As a result, there is no basis to restrict carriers' data retention.

### **III. COMPREHENSIVE OPT-IN REQUIREMENTS ARE UNECESSARY AND WOULD VIOLATE THE FIRST AMENDMENT.**

In addition to addressing the topics contained in the Commission's *2007 CPNI Order*, the Consumer Coalition rehashes an argument from EPIC's April 14, 2006 comments and argues that the Commission's *2007 CPNI Order*, which requires opt-in consent only with respect to a carrier's joint venture partners or independent contractors, should be extended to agents and affiliates.<sup>46</sup> Yet the Consumer Coalition offers no new evidence and ignores the Commission's rationale for requiring opt-in consent set forth in its *2007 CPNI Order*. There, the Commission sought to allow customers to regulate their carrier's sharing of their CPNI with joint venture partners or independent contractors because "the carrier no longer has control over it and thus the

---

<sup>41</sup> See 47 C.F.R. § 42.6-.7.

<sup>42</sup> See, e.g., NYCRR16 § 651.19.54.

<sup>43</sup> 15 U.S.C. § 1681 *et seq.*

<sup>44</sup> See, e.g., Comments of Verizon at 18; Comments of Sprint Nextel at 16-18; Comments of T-Mobile at 7.

<sup>45</sup> Comments of Consumer Coalition at 22.

<sup>46</sup> *Id.* at 22.

potential for loss of this data is heightened.”<sup>47</sup> This rationale would not apply to CPNI shared with agents and affiliates. Rather, opt-out consent is appropriate in those instances despite any burden on consumers to exercise their opt-out rights because “many customers accept and understand that carriers will share their information with affiliates and agents.”<sup>48</sup>

Thus, the Commission did not change its opt-out rules for affiliates and agents since doing so would run counter to customer expectations, would increase marketing costs (which ultimately would be borne by customers), and would do nothing to address the data brokering issue. Furthermore, a comprehensive opt-in requirement would directly infringe the ability of carriers to engage in protected commercial speech in violation of the First Amendment.<sup>49</sup>

Contrary to the Consumer Coalition’s claims, customers expect that, having entered into a customer-carrier relationship, their data will be used by their carrier to offer them discounts and market new service offerings. Information about usage patterns enables carriers to tailor marketing to a consumer’s needs, improving efficiency.<sup>50</sup> At the same time, contrary to the claims of the Consumer Coalition,<sup>51</sup> the practice reduces inefficient and unwanted advertising,

---

<sup>47</sup> 2007 CPNI Order ¶ 39.

<sup>48</sup> *Id.* ¶ 40.

<sup>49</sup> See *Requiring “Opt-In” Prior to Sharing CPNI with Marketing Vendors: Unconstitutional and Unwise*, white paper attached to Verizon letter, CC Docket No. 96-115, (Jan. 29, 2007); Verizon letter, CC Docket No. 96-115 (Dec. 22, 2006); see also *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999); *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, 17 FCC Rcd 14860 (2002) (“*Third Report and Order*”).

<sup>50</sup> *Id.* ¶ 35 (citing Letter from Michael D. Alarcon, SBC, to William Caton, Acting Secretary, Federal Communications Commission, CC Docket Nos. 96-115 and 96-149 (filed April 12, 2002) (stating that interim opt-out approval has resulted in “[c]ustomized offerings of SBC’s products and services based on customers’ CPNI”).

<sup>51</sup> Comments of Consumer Coalition at 10.

enhancing consumer privacy.<sup>52</sup> If comprehensive opt-in consent were required, it is likely that carriers would find opt-in consent too costly to implement and thus send mass mailings to all customers, rather than just those customers whose CPNI indicates that they may be interested in the offerings. Indeed, it is not surprising that customers want to receive targeted notices regarding carrier service offerings as they expect to benefit from them.<sup>53</sup>

By contrast, an opt-in requirement frustrates consumer expectations and increases costs to carriers and consumers without improving existing safeguards against data brokers. As the Commission previously has found, opt-in – requiring affirmative customer approval prior to use of data for marketing – deprives consumers of commercial information they desire to receive.<sup>54</sup> For example, an opt-in requirement might prevent a carrier from marketing to a consumer a bundle of services – including services to which the consumer does not currently subscribe – that would reduce the costs of existing services while adding desired new services. Such a requirement also would increase the cost of targeted marketing campaigns – costs ultimately borne by consumers in higher rates – and result in more unwelcome marketing to consumers.

Moreover, opt-in burdens consumers and increases costs while adding nothing to existing safeguards on customer data. There is no evidence that data brokers are targeting agents or affiliates, know the identity of these entities, and are more successful in achieving unauthorized access from them. Even if there were, an opt-in regime would not inhibit pretexters' ability to use deception and impersonation to get access to CPNI. Opt-in/opt-out regimes relate to the

---

<sup>52</sup> *Third Report and Order* ¶ 35 (citing AT&T Comments at 5, n.3 (“Indeed, limiting the use of CPNI may have the effect of increasing the number of solicitations by telecommunications carriers.”)).

<sup>53</sup> *Id.* ¶ 35 (citing Letter from Gina Harrison, Pacific Telesis Group, to William F. Caton, Acting Secretary, Federal Communications Commission, CC Docket No. 96-115 (Dec. 12, 1996), Attach. A at 8 (“Westin Survey”)).

<sup>54</sup> *Id.* ¶¶ 35-36.

authorization required before companies may use CPNI, not the level of protection such information is afforded. Customers who do not exercise their opt-out rights are as secure from data broker activity as those who do.

In addition, opt-in burdens protected commercial speech in contravention of the First Amendment. As Verizon has previously explained, the Tenth Circuit concluded that the FCC failed to carry its burden of demonstrating opt-in authorization both materially advanced a governmental interest in protecting consumer privacy and was narrowly tailored to restrict no more speech than necessary to achieve that purpose.<sup>55</sup> On remand, the Commission adopted an opt-out rule after concluding that, despite extensive fact gathering and record development, it could not articulate a constitutional basis for requiring opt-in.<sup>56</sup> The Federal District Court for the Western District of Washington followed the same approach as the Tenth Circuit and the FCC in striking down a Washington State opt-in rule on First Amendment grounds.<sup>57</sup>

The Commission is cognizant of this precedent and explained in its *2007 CPNI Order* why it believes that requiring opt-in consent for CPNI disclosures to joint venture partners and independent contractors is constitutional under the Supreme Court's *Central Hudson*<sup>58</sup> test for commercial speech.<sup>59</sup> The Commission set forth specific findings, the following three of which are based on CPNI leaving the control of the carrier:

(3) the more independent entities that possess CPNI, the greater the danger of unauthorized disclosure;

---

<sup>55</sup> See Reply Comments of Verizon (June 2, 2006) at 5 (citing *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999)).

<sup>56</sup> See *Third Report and Order*, Statement of Chairman Michael K. Powell at 1.

<sup>57</sup> *Verizon Northwest, Inc. v. Showalter*, 282 F. Supp. 2d 1187 (W.D. Wash. 2003).

<sup>58</sup> *Central Hudson Gas & Elec. v. Public Serv. Comm'n*, 447 U.S. 557 (1980).

<sup>59</sup> *2007 CPNI Order* ¶ 45.

(4) an opt-in regime directly and materially advances privacy and safety interests by giving customers direct control over the distribution of their private information outside the carrier-customer relationship; and

(5) an opt-in regime is not more extensive than necessary to protect privacy and safety interests because opt-out rules . . . do not adequately secure customers' consent for carriers to share CPNI with unaffiliated entities.<sup>60</sup>

None of these findings would apply to CPNI disclosures to affiliates and agents. In the absence of evidence of an elevated risk to CPNI when disclosed to a carrier's agents or affiliates, which the Consumer Coalition fails to provide, a comprehensive opt-in requirement would be more extensive than necessary and thus violate the First Amendment.

Finally, the Consumer Coalition suggests an alternative to comprehensive opt-in – i.e., requiring carriers to identify every affiliate, agent or entity to whom CPNI has been disclosed for marketing purposes on a customer's monthly billing statement.<sup>61</sup> Yet such a requirement has no relation to the data broker problem that the Commission is attempting to address in this proceeding. It is unrealistic to expect that upon receipt of this information, customers would be able to ascertain which of the listed agents and affiliates do not employ the appropriate data security practices to thwart data brokers and then opt-out. Moreover, this proposal would add substantial clutter to bills, especially when a carrier has a complex corporate structure with a number of affiliates. If the Consumer Coalition is truly worried about imposing transaction costs on customers, this proposal cannot be justified. In addition, implementing this scheme would be costly for the companies who prepare these bills for customers as new systems and processes

---

<sup>60</sup> *Id.*

<sup>61</sup> Comments of Consumer Coalition at 24.

would be required. And this too presents a constitutional problem because compelled speech enjoys First Amendment protection.<sup>62</sup>

Accordingly, the Consumer Coalition provides no compelling reason for the Commission to revisit its *2007 CPNI Order*, which requires opt-in consent only for CPNI shared with joint venture partners and independent contractors for marketing.

#### **IV. CONCLUSION**

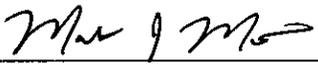
It is clear that the Consumer Coalition's assertion that its proposals would "carry substantial benefits to carriers both large and small"<sup>63</sup> lacks any evidentiary support in light of the well-established burdens. The Consumer Coalition simply assumes its conclusion – i.e., that extensive breaches that are costly to remedy would occur in the absence of further regulation – while failing to tie its proposals to remedying the data broker problem that is the basis of this proceeding. Therefore, until the Commission can evaluate the efficacy of its newly enacted rules, it should reject proposals to require: (1) passwords for non-call detail CPNI provided in response to customer-initiated calls; (2) audit trails; (3) encryption; and (4) data deletion after a certain time. The same restraint should apply to the renewed proposal for comprehensive opt-in requirements.

---

<sup>62</sup> See, e.g., *Riley v. Nat'l Fed'n of the Blind of N.C., Inc.*, 487 U.S. 781 (1988).

<sup>63</sup> Comments of Consumer Coalition at 1.

Respectfully submitted,

By: 

---

Karen Zacharia  
Mark J. Montano  
VERIZON  
1515 N. Court House Road  
Suite 500  
Arlington, VA 22201-2909  
703.351.3058

Of Counsel  
Michael E. Glover

Counsel for Verizon

Dated: August 7, 2007