

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the	)	CC Docket No. 96-115
Telecommunications Act 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 QWEST COMMUNICATIONS INTERNATIONAL INC.**

Craig J. Brown  
Kathryn Marie Krause  
Suite 950  
607 14<sup>th</sup> Street, N.W.  
Washington, DC 20005  
303-383-6651

Attorneys for

QWEST COMMUNICATIONS  
INTERNATIONAL INC.

August 7, 2007

## TABLE OF CONTENTS

	Page
I. INTRODUCTION AND SUMMARY: NO FURTHER CPNI RULE AMENDMENTS ARE NECESSARY.....	1
II. CA, <i>ET AL.</i> AND NJ RATE COUNSEL FAIL TO DEMONSTRATE A NEED FOR ADDITIONAL GOVERNMENT REGULATION OF CPNI.....	5
A. Additional Password Requirements Are Unnecessary, Would Be Unwelcome By Consumers, And Would Increase The Cost Of Providing Service Exorbitantly. ....	5
B. A Commission Mandate That Carriers’ Customer Information Be Encrypted In Storage Would Entail Huge Costs And Be Discriminatory.....	11
C. The Commission Should Not Intrude Into The Business Operations Of Carriers By Mandating Particular Audit Capabilities Or Programs. ....	14
D. The Commission Should Not Prescribe Data Retention Or Destruction Timeframes Because Doing So Interferes With Reasonable Business Operations and Data Retention Programs. ....	16
E. It Is Premature For The Commission To Prescribe “Information-Deletion” Functionalities For Mobile Phone Equipment, Since The Market Continues To Create And Offer Such Functionality. ....	18
F. CA, <i>Et Al.</i> Fails To Demonstrate A Need For Its Other Proposed Government Mandates.....	19
III. CONCLUSION .....	21

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the	)	CC Docket No. 96-115
Telecommunications Act 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 QWEST COMMUNICATIONS INTERNATIONAL INC.**

**I. INTRODUCTION AND SUMMARY: NO FURTHER CPNI RULE AMENDMENTS ARE NECESSARY.**

Of the 30 commenting parties in this proceeding, only two argue for the promulgation of additional federal rules regarding access, use and disclosure of Customer Proprietary Network Information ("CPNI") -- Consumer Action, *et al.*<sup>1</sup> and New Jersey Rate Counsel.<sup>2</sup> Both parties advocate through conclusions; and neither presents supporting empirical evidence. On more than one occasion, CA, *et al.* improperly seeks to insinuate issues into this proceeding that are beyond the scope of the instant *Further Notice*.<sup>3</sup>

---

<sup>1</sup> See Comments of Consumer Action, Consumer Federal of America, Consumers Union, Electronic Privacy Information Center, National Consumers League, Privacy Activism, Privacy Journal, Privacy Rights Clearinghouse, U.S. Public Interest Research Groups, Utility consumers' Action Network ("CA, *et al.*"), filed July 9, 2007.

<sup>2</sup> See Comments of the New Jersey Division of Rate Counsel ("NJ Rate Counsel"), filed July 9, 2007.

<sup>3</sup> See *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115 and WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22, 22 FCC Rcd 6927, rel. Apr. 2, 2007 ("*April 2007 CPNI Order*" or "*Further Notice*" as appropriate). Comments were filed July 9, 2007.

But by far the most fatuous advocacy is that of CA, *et al.* with its completely groundless argument that additional CPNI rules would really be “good for carriers,”<sup>4</sup> despite carriers’ protestations to the contrary. Of course, CA, *et al.* are in no position to espouse the benefits of additional federal regulations for affected carriers, and their mission is not aligned with such an objective. They promote what they purport to be “consumer” interests, ignoring downstream costs to those consumers and eschewing the notion that carrier regulatory burdens bear any relevance to carrier-consumer relationships or the public policy associated with them.<sup>5</sup> Essentially, their views about carrier operations, costs, and putative efficiencies are nothing but uninformed.

Absent from the advocacy of either proponent of expanded regulation is any meaningful, disciplined cost-benefit analysis that would shed light on the true cost burden that consumers would bear should the Federal Communications Commission (“Commission”) enact the overreaching rules the commentors propose. The costs would be enormous; the benefits would be at best marginal and more likely illusive. For all these reasons, the Commission should reject their proposals.

Based on the numerous and varied infirmities in the arguments of those pressing for additional regulation of CPNI access and disclosure, Qwest urges the Commission to reject the arguments. More compelling than the positions of CA, *et al.* and NJ Rate Counsel are the

---

<sup>4</sup> CA, *et al.* argues that carriers should welcome additional rules and regulations defining, limiting, and affecting their relationships and communications with their customers. Such rules, CA, *et al.* claims, are a boon to carriers both large and small (CA, *et al.* at 1), because such rules are the equivalent of good business decisions and would operate to protect corporate reputations. CA, *et al.* advances this argument in support of government-mandated passwords for access to all CPNI. *Id.* at 7.

<sup>5</sup> For example, CA, *et al.* at 10 cites to Qwest’s April 28, 2006 Comments, CC Docket No. 96-115 at 10-13 (“Qwest 2006 Comments”). For purposes of this filing, Qwest means Qwest Communications International Inc., the parent company of Qwest’s common carrier operations.

arguments of the overwhelming number of commenting service providers who persuasively argue that no additional CPNI rules are necessary. Among the reasons cited are:

- Carriers need some time to implement the new CPNI rules before seriously considering adding new rules.<sup>6</sup>
- The Commission should review the data in the carrier reports it has now required be submitted before promulgating any additional rules.<sup>7</sup>
- Recent legislation making pretexting activity criminal renders additional regulation in this area premature.<sup>8</sup>
- Service providers necessarily take protective measures regarding their customer information because the marketplace, and consumer confidence, require it.<sup>9</sup>
- Where carriers fail to take appropriate and reasonable precautions regarding CPNI, the Commission has enforcement actions available.<sup>10</sup>
- Any additional rules could impose substantial burdens on consumers without any commensurate benefits.<sup>11</sup>
- Based on experience, pretexters want to know who customers call, not information regarding the types of service they purchase, their repair histories or their general billing information.<sup>12</sup>
- Non-call detail CPNI is not particularly sensitive<sup>13</sup> and is in high demand with consumers.<sup>14</sup>

---

<sup>6</sup> See, e.g., AT&T Inc. at 3-4 (“AT&T”); Comcast Corporation at 6 (“Comcast”); COMPTTEL at 2-3; National Telecommunications Cooperative Association at 2-3 (“NTCA”); National Cable & Telecommunications Association at 2 (“NCTA”); Sprint Nextel Corporation at 5-6 (“Sprint Nextel”); Time Warner Inc. at 6 (“Time Warner”); T-Mobile USA, Inc. at 2-4, 6 (“T-Mobile”); Vonage Holdings Corporation at 2-3 (“Vonage”).

<sup>7</sup> See, e.g., AT&T at 3-4.

<sup>8</sup> See, e.g., Time Warner at 5; Sprint Nextel at 18; Verizon at 18.

<sup>9</sup> See, e.g., Comcast at 8.

<sup>10</sup> See, e.g., AT&T at 8.

<sup>11</sup> See, e.g., AT&T at 5; Comcast at 4.

<sup>12</sup> See, e.g., AT&T at 5; Independent Telephone and Telecommunications Alliance at 2-3 (“ITTA”); Verizon at 9.

<sup>13</sup> See, e.g., Time Warner at 7.

- Carriers are well equipped to respond to customer demands for passwords, and customers are the best party to determine if they are needed.<sup>15</sup>
- Mandatory passwords would subject the customer contact process to longer customer service call times, delayed access to information, and increased customer dissatisfaction.<sup>16</sup>
- Mandatory passwords implicate constitutional protections and would be unlawful based on the current record.<sup>17</sup>
- Encryption-in-storage of CPNI bears little relation to pretexting or its prevention.<sup>18</sup>
- No encryption-in-storage government mandate can pass a reasoned cost-benefit analysis.<sup>19</sup>
- There is no demonstration that carrier audit trails would prevent or stop those intent on misappropriating information from service providers.<sup>20</sup>
- A variety of complex federal and state laws influence a service provider's data retention program and the Commission should not interfere with those programs.<sup>21</sup>
- The record fails to suggest any relationship between data retention and pretexting and the Commission should not generally regulate in this area.<sup>22</sup>
- No government mandate prescribing particular audit controls can pass a reasoned cost-benefit analysis.<sup>23</sup>

---

<sup>14</sup> See, e.g., Sprint Nextel at 7; Verizon at 8-9.

<sup>15</sup> See, e.g., AT&T at 6-7; Time Warner at 7.

<sup>16</sup> See, e.g., Comcast at 4; Frontier Communications at 4-5 ("Frontier"); NuVox Communications and XO Communications LLC at 3-4 ("NuVox and XO"); NCTA at 3 (noting particular frustration with passwords for certain groups of customers, such as senior citizens, persons with disabilities, and non-English speaking persons); USTA at 3-4; Verizon at 3-4.

<sup>17</sup> See, e.g., Verizon at 10-11.

<sup>18</sup> See, e.g., Sprint Nextel at 14-15; Verizon at 15-17.

<sup>19</sup> See, e.g., Embarq at 3; MetroPCS Communications, Inc. at 9-10 ("MetroPCS"); Sprint Nextel at 11-12.

<sup>20</sup> See, e.g., Embarq at 3; Rural Cellular Association at 3-4; Sprint Nextel at 10-11; T-Mobile at 7; Verizon at 16.

<sup>21</sup> See, e.g., Comcast at 8-9; NuVox and XO at 7-8; Sprint Nextel at 16, 18-19; Verizon at 17-20.

<sup>22</sup> See, e.g., MetroPCS at 10; Time Warner at 11-12.

- Consumers have tools and carriers act reasonably and responsibly with regards to the removal of personal information from cellphones.<sup>24</sup>

For the litany of reasons outlined above, Qwest agrees with those carriers arguing that no additional CPNI rules are required. Unless the Commission is faced with a particular carrier that has demonstrably failed to take reasonable means to protect information about its customers, the Commission should defer to the reasoned judgment of businesses on the management and security of customer information.

## **II. CA, *ET AL.* AND NJ RATE COUNSEL FAIL TO DEMONSTRATE A NEED FOR ADDITIONAL GOVERNMENT REGULATION OF CPNI.**

### **A. Additional Password Requirements Are Unnecessary, Would Be Unwelcome By Consumers, And Would Increase The Cost Of Providing Service Exorbitantly.**

CA, *et al.* and NJ Rate Counsel argue for a government mandate that passwords must be used before a customer can access or a carrier can disclose any CPNI, even to the customer who is the subject of the information. Their argument here, like CA, *et al.*'s argument about what is "good for carriers," is at odds with the constituency they claim to represent because consumers do not like passwords.<sup>25</sup> A government mandate forcing customers to use passwords would be hostile, not friendly, regulation.

In addition to the off-base assumption about consumer receptivity to passwords, CA, *et al.* makes other unproven assumptions: (1) that general telephone account CPNI is comparably

---

<sup>23</sup> See, e.g., T-Mobile at 2-5; USTA at 4-5.

<sup>24</sup> See, e.g., AT&T at 9-11; Embarq at 5; Sprint Nextel at 22-23; T-Mobile at 8.

<sup>25</sup> See *April 2007 CPNI Order* at n.47, finding that consumers may not like passwords and citing positively AT&T's 2006 Comments at 8-11 (AT&T referenced a Ponemon Institute study showing that the vast majority of respondents opposed the use of passwords; see Larry Ponemon, PhD, Data Security, Study on Passwords Reveals Most Forget, Must Reset Passwords Multiple Times, *Privacy & Security Law*, Vol. 5, No. 10 (March 6, 2006) at 8-9 and Centennial's 2006 Comments at 3-4. *And see* AT&T at 5; Verizon at 5-6 and nn.5-8.

sensitive to call detail; and (2) that consumers will be harmed absent additional CPNI password requirements. Both assumptions are incorrect. The first of these two assumptions is logically not evident; the second at most speculative,<sup>26</sup> especially in light of the changes required by the most-recently adopted rules.

But the initial inquiry into whether the Commission should mandate passwords for all CPNI should start with consumers' preferences and receptivity to such a regime. *CA, et al.* does not address the Commission's factual observation that consumers do not like passwords.<sup>27</sup> Consumers have difficulty with passwords because they are hard to remember and make transactions more complicated.<sup>28</sup> The empirical survey evidence in the existing record is left unrebutted by *CA, et al.* Moreover, the record evidence resonates with common consumer experience, not only of those persons drafting comments in this proceeding but those contemplating additional regulations in this area. Simply put, multiple passwords with multiple vendors is a pain. Passwords must be tracked; and often consumers forget or lose passwords. The consequence of all this is that passwords create an absolute barrier to speech in some circumstances or create hoops that must be jumped through in order to engage in even routine commercial communications. In all cases, passwords exact a considerable toll on efficient and satisfying communication. Absent evidence that some compelling need requires such a barrier to

---

<sup>26</sup> See NJ Rate Counsel at Section IV (arguing that restricting "password requirements to call records *may be* insufficient and fall short" (emphasis added)). In addition, *CA, et al.* speculates that there may be some connection between non-call detail CPNI and pretexting -- something it never proves. *And see* notes 30 and 32 and 33, *infra*.

<sup>27</sup> See note 25, *supra*. NJ Rate Counsel claims that carrier arguments against the extension of password protection to generally insensitive CPNI are "simplistic notions" and that there is no empirical evidence suggesting that consumers would not embrace additional password protection. NJ Rate Counsel at Section V. NJ Rate Counsel is incorrect. As noted above, the record reflects, and the Commission has previously acknowledged, that consumers do not favor passwords.

<sup>28</sup> See, e.g., AT&T at 5; Verizon at 5-6 and nn.5-8.

easy carrier-customer communications, such regulation would be unlawful.<sup>29</sup> *CA, et al.* never provides such evidence, compelling or otherwise.

Nor do those claiming that all CPNI is equally sensitive prove their claims.<sup>30</sup> It seems obvious that not all elements of CPNI are equally sensitive, or as sensitive as call detail records - the focus of misappropriation by pretexters.<sup>31</sup> The fact that a customer has custom calling or CLASS features, or purchases two lines in a bundled package, is not sensitive account

---

<sup>29</sup> Proponents of a mandatory-password regime also ignore the fact that CPNI is also carrier business information. To restrict a carrier from using its own records to craft communications to its customers and respond to customer inquiries requires the identification of a substantial harm seeking to be avoided and a compelling governmental interest sought to be achieved. *US WEST v. FCC*, 182 F.3d 1224, 1235 (10th Circuit 1999). The proponents prove neither.

<sup>30</sup> *Compare* NJ Rate Counsel at Section V. (recommending “that the rationale of the existing rules logically extend to the expansion of CPNI protections to non-call detail”). NJ Rate Counsel never explains the logical progression, however. *And see id.* (arguing -- with no evidence -- that “[n]on-call detail contains sensitive personal information, which is just as worthy for protection from those looking to obtain such information for improper purposes”). NJ Rate Counsel never demonstrates that others seek to obtain such information for improper purposes.

*CA, et al.* argues, obliquely, that the Commission should mandate passwords for CPNI access because customers do not understand the term CPNI or appreciate the privacy implications associated with such information. *CA, et al.* at 7. Qwest sees no relation between *CA, et al.*’s observation and a need to impose mandatory passwords on account access. On the contrary. The latter observation implies that there may be no appreciable privacy concern regarding such information.

<sup>31</sup> The Commission has classified customer information as belonging to three broad categories according to sensitivity: individually-identifiable CPNI, aggregated CPNI and subscriber list information (“SLI”). *See, e.g., Further Notice*, 22 FCC Rcd at 6930 n.7 (2007). The Commission characterized individually-identifiable CPNI as the most “sensitive” within these categories. And while the Commission has referred to the entire category of individually-identifiable CPNI as “sensitive” information, a review of its statements makes clear that the Commission considered call detail the “most sensitive” of all individually-identifiable CPNI. The *1998 CPNI Order* notes that “CPNI includes information that is extremely personal to customers . . . such as to whom, where and when a customer places a call,” and observes that “call destinations and other details about a call . . . may be equally or more sensitive [than the content of the calls].” *1998 CPNI Order*, 13 FCC Rcd 8064-65 ¶ 2, 8132-33 ¶ 94.

While the Tenth Circuit generally accepted the Commission’s stratification approach to CPNI sensitivity, it did note that the Commission had “summarily” determined that call detail information was “sensitive” and later characterized individually-identifiable CPNI as “allegedly sensitive information.” *See US WEST v. FCC*, 182 F.3d at 1235.

information. Nor, to the best of Qwest's knowledge, have pretexters sought such information in any numbers.<sup>32</sup> Moreover, such information is unlikely to form an evidentiary foundation for "identity theft" -- a red herring argument repeatedly raised by CA, *et al.*<sup>33</sup> Information that "relates to the quantity, technical configuration, type . . . and amount of use of a telecommunications service"<sup>34</sup> is not likely to assist a bad actor intent on assuming another's identity. And CA, *et al.* never proves otherwise.

Not only do supporters of mandatory passwords fail to prove the need for them or their desirability, but they continue to significantly understate the tasks and cost burden associated with implementing such a regime<sup>35</sup> -- costs which the record shows would be exorbitant<sup>36</sup> and inevitably passed onto consumers.<sup>37</sup> Moreover, they fail to explain why telecommunications

---

<sup>32</sup> See CA, *et al.* suggesting -- with no proof -- that access to non-call detail CPNI "opens a loophole for pretexters to exploit." *Id.* at 7.

<sup>33</sup> See *id.* at 2 (noting that the Federal Trade Commission ("FTC") has listed identity theft as a major consumer complaint), but never examining -- let alone explaining -- the relationship between pretexters attempting to secure information from telecommunications companies and identity theft; nor articulating how CA, *et al.*'s suite of "protections" would meaningfully protect against identity theft where carrier information most likely plays no part. *And see* pages 14-16 and nn. 59, 61 and 63, *infra*.

<sup>34</sup> 47 U.S.C. § 222(h)(1)(A).

<sup>35</sup> CA, *et al.* claims that "[c]arriers can easily implement [a mandatory password] rule, as it would require minimal staffing." CA, *et al.* at 7. While the former (easy implementation) is just wrong, what it has to do with the latter is unclear. Is CA, *et al.* suggesting that carriers can lay off employees that now engage in customer verification, or that only minimal additional staffing would be required to deploy such a regime? Other comments suggest the former.

<sup>36</sup> See, e.g., Verizon at 8; Time Warner at 6.

<sup>37</sup> NJ Rate Counsel, for example, is under the assumption that the Commission's previous CPNI prescriptions do "not impos[e] the burdens of such rules on consumers." NJ Rate Counsel at Section III. This is clearly incorrect. All of the systems changes and practice changes associated with customer-carrier interaction entail substantial costs that will clearly be borne by customers of carriers. The fact that such costs are incorporated into the cost of goods sold, rather than a specific "regulatory surcharge" does not mean that consumers do not bear the cost burden. *And see* CA, *et al.* at 10 suggesting somewhat cheekily that a carrier's cost-benefit analysis is self-serving and cannot reflect the public interest. But since a carrier's costs of implementing any

service providers should be the target for such massive cost burden or unprecedented regulatory intervention in their provider-customer relationships.

Surely telecommunications data is not more sensitive than financial or medical data, but the government has not mandated passwords in the context of those supplier-consumer communications. Additionally, a mandatory password requirement for “all CPNI” perniciously discriminates between those companies with substantial CPNI and those with only a little.

The history and business model of traditional common carriers means that a substantial amount of the customer information in their possession is statutorily-defined CPNI.<sup>38</sup> On the other hand, new entrants have other customer information, like cable subscriber information,<sup>39</sup> and are only just now collecting and storing CPNI. And cable companies are free to collect and use their cable subscriber information in connection with other ancillary services, such as wire services (*i.e.*, telephony) or radio services, unhampered by any mandatory password requirement.<sup>40</sup>

Customers could become so irritated with companies who persistently demand passwords before discussing CPNI account information (*e.g.*, traditional telcos) that they might take their business elsewhere where such password information is only asked for in a very limited context (*e.g.*, cable companies). This is not a competitively neutral regulatory model. Accordingly, it should be avoided.

---

federal mandate are necessarily passed on to consumers, if the attendant consumer benefit is not greater than a carrier’s costs the consumer *does not* benefit.

<sup>38</sup> See 47 U.S.C. § 222(h)(1) for the statute definition of CPNI; *and see also* 47 C.F.R. § 64.2003(d).

<sup>39</sup> See 47 U.S.C. § 551.

<sup>40</sup> *Id.* at § 551(a)(2)(B), (b)(2).

At the same time as *CA, et al.* and NJ Rate Counsel argue for more extensive government regulation in the nature of mandatory passwords to access any CPNI, neither proponent address the legality of such regulation. Their failure to address this issue is fatal to their advocacy generally and, more specifically, to their articulation of the public interest.<sup>41</sup>

An “all CPNI” mandatory password regime would suppress protected speech between carriers and their customers, often with respect to routine account matters where non-sensitive information was to be discussed. The proponents of such a regime must identify a compelling governmental interest to support such regulation, which they fail to do, especially an interest that would be confined to telecommunications carriers. There is no such compelling interest.<sup>42</sup>

All told, both *CA, et al.* and NJ Rate Counsel fail to demonstrate how their proposal for mandatory passwords would be in the consumer’s best interests.<sup>43</sup> They fail to show that

---

<sup>41</sup> *US WEST v. FCC*, 182 F.3d at 1228 (the review of the Commission’s 1998 *CPNI Order* (13 FCC Rcd 8061, rel. Feb. 26, 1998) presented a “case [which was considered] a harbinger of difficulties encountered in this age of exploding information, when rights bestowed by the United States Constitution must be guarded as vigilantly as in the days of handbills on public sidewalks. In the name of deference to agency action, important civil liberties, such as the *First Amendment’s* protection of speech, could easily be overlooked.”).

<sup>42</sup> *See US WEST v. FCC*, 182 F.3d at 1235 (“In the context of a speech restriction imposed to protect privacy by keeping certain information confidential, the government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another’s identity.”).

<sup>43</sup> It is not sufficient to argue that consumers do not know or appreciate the privacy implications associated with CPNI (*see CA, et al.’s* argument at note 30, above) or fail to request passwords when they should. *Compare* the Tenth Circuit’s observation that the Commission and its supporters “merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.” *US WEST v. FCC*, 183 F.3d at 1249. The same can be said of passwords. The government cannot impose passwords based on the argument that consumers do not know how to act in their own best interests when it comes to making choices about having passwords. Protectionist notions are insufficient to constitute a compelling interest in support of restrictions on commercial speech. *See Virginia State Bd. of Pharmacy v. Virginia Citizens*

consumers would tolerate (let alone embrace) mandatory password requirements for access to all CPNI. They fail to show that a cost-benefit analysis would support the imposition of such passwords. And they fail to show that a government prescription for mandatory passwords to access all CPNI would be constitutional.

In contrast to its opposition to CA, *et al.* and NJ Rate Counsel, Qwest supports those service providers speaking on their own behalf that oppose mandatory passwords because they are: (a) ill-suited to address the matter of pretexting beyond access to call-detail information;<sup>44</sup> (b) burdensome from a cost perspective for both carriers and customers alike;<sup>45</sup> (c) burdensome from a communications perspective for both carriers and customers alike (rendering the constitutionality of such a regime highly doubtful);<sup>46</sup> and (d) burdensome from a parity perspective with respect to carriers and other commercial enterprises.<sup>47</sup>

**B. A Commission Mandate That Carriers' Customer Information Be Encrypted In Storage Would Entail Huge Costs And Be Discriminatory.**

CA, *et al.* devotes but two scant paragraphs in support of a government regulation requiring encryption of CPNI in storage. In the most coy of understatements, CA, *et al.* notes that such endeavor "may be costly."<sup>48</sup> CA, *et al.*'s lack of certainty regarding the magnitude of

---

*Consumer Council, Inc.*, 425 U.S. 748, 769 (1976); *Edenfield v. Fane*, 507 U.S. 761, 767 (1993); *44 Liquormart, Inc. v. Rhode Island*, 116 S. Ct. 1495, 1507 (1996) (principal opinion).

<sup>44</sup> See, e.g., AT&T at 5; ITTA at 2-3; Verizon at 9; Comcast at 4; Frontier at 4-5; NuVox and XO at 3-4; NCTA at 3; USTA at 3-4; Verizon at 3-4.

<sup>45</sup> See, e.g., NuVox and XO at 2, 3; Sprint Nextel at ii; Comcast at 6; ITTA at 3; Verizon at 3, 5-6; ICORE at 3-4.

<sup>46</sup> See, e.g., NuVox and XO at 3; T-Mobile USA at 3-4; Comcast at 4-5; MetroPCS at 5; Time Warner at 8; Frontier at 3-5; ITTA at 3; USTA at 3.

<sup>47</sup> See, e.g., Comments of American Association of Paging Carriers at 3.

<sup>48</sup> CA, *et al.* at 10.

costs likely attendant to its proposal is startling, given that the record reflects that it would cost millions and millions of dollars to implement a CPNI encryption-in-storage program.<sup>49</sup>

Furthermore, under CA, *et al.*'s view, its government-mandated "encryption in storage" regime would apply only to telecommunications service providers. Strikingly, it would be discriminatory by design and nature. Not only would such a regulatory scheme obviously discriminate between telecommunications providers and other retail establishments, it would create a discriminatory competitive environment between traditional telecommunications companies and new entrants, such as cable companies, similar to that which could occur with a mandatory-password regulation.<sup>50</sup> New entrants would have little CPNI they would be "forced" to encrypt in storage in the event of such a government mandate, while traditional telephone companies would have a great deal of information to encrypt. Clearly, such a regulatory regime would not be competitively neutral either in its scope or cost burden. For this reason alone, it should be rejected.

Rather than tackle or rebut the existing record evidence of the cost burden that traditional carriers would suffer were the Commission to adopt an encryption-in-storage regime, CA, *et al.* makes two tangential arguments. Neither is convincing. First, CA, *et al.* asserts that the FTC recommends that businesses consider encryption of sensitive information,<sup>51</sup> with the suggestion that the Commission follow suit. It is true that the FTC has made such a recommendation with

---

<sup>49</sup> See Qwest 2006 Comments at n.19 citing to Comments of Verizon, RM-11277, filed Oct. 31, 2005 at 4-5, wherein Verizon predicted that the costs just for EPIC's document retention and encryption proposals would "likely . . . cost the industry hundreds of millions of dollars to develop and implement." *And see* Comments of Alltel Corporation, CC Docket No. 96-115, filed Apr. 28, 2006 at n.17 ("Alltel 2006 Comments"); Comments of BellSouth Corporation, CC Docket No. 96-115, filed Apr. 28, 2006 at 17 n.35, 18 ("BellSouth 2006 Comments").

<sup>50</sup> See Section II.A., *supra*.

<sup>51</sup> CA, *et al.* at 10.

respect to sensitive information.<sup>52</sup> But the FTC does not mandate such encryption. Should the Commission be inclined, it too could make a recommendation that businesses consider using encryption when they store sensitive information. Such a general recommendation would allow businesses to implement the recommendation in a manner appropriate to a particular business's operational needs, technical infrastructure and risk levels. But, like the FTC, the Commission should take no prescriptive action.

Second, *CA, et al.* makes the point that carriers usually encrypt sensitive data in transmission and when customers view such information online. This is also true, but is irrelevant in support of *CA, et al.*'s claim that customer information should be encrypted in storage. The encryption of confidential information in transit, including customer information, is a widespread commercial practice by retailers (and others), as is evident by the evidence already in the record.<sup>53</sup> But the significant features and elements associated with encryption of information "in transit" versus encryption "in storage" are very different. Each activity has different technical requirements, cost structures and legal implications.<sup>54</sup> Demonstrating that one is commonplace (*i.e.*, encryption in transit) proves nothing about the cost-benefit of the other (*i.e.*, encryption in storage) or its promotion of the public interest. The Commission should reject any CPNI encryption-in-storage requirement.

---

<sup>52</sup> [www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf](http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf) (viewed Aug. 6, 2007).

<sup>53</sup> See Qwest 2006 Comments at 12, 29; Comments of RNK Inc. d/b/a RNK Telecom, CC Docket No. 96-115, RM-11277, filed April 28, 2006 at 6.

<sup>54</sup> See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 110 Stat. 1848 (as codified at 18 U.S.C. § 2510 *et seq.*), with respect to the different standards for interception of information in transit versus information "in storage".

**C. The Commission Should Not Intrude Into The Business Operations Of Carriers By Mandating Particular Audit Capabilities Or Programs.**

CA, *et al.* says nothing substantively different than one of its members, the Electronic Privacy Information Center (“EPIC”), said in its original Petition<sup>55</sup> or its Reply Comments.<sup>56</sup> But it goes too far in describing the state of carrier audit controls generally and in its request for additional prescriptions.

CA, *et al.* claims, but clearly cannot prove, that “most carriers own the infrastructure required to record *all attempts to access a customer’s record*, reducing the burden on implementing this system.”<sup>57</sup> Only a commentator totally uneducated by the existing record could make such a wrong statement. Carriers do not currently have audit features that would track “all” access to customer information. Nor do they think such systems are necessary or appropriate judged by any rational cost-benefit analysis.<sup>58</sup> And while a journalist might find sophisticated audit features that incorporate algorithms interesting, at least with respect to the

---

<sup>55</sup> Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115, filed Aug. 30, 2005 (“EPIC Petition”).

<sup>56</sup> Reply Comments of the Electronic Privacy Information Center, CC Docket No. 96-115, filed June 2, 2006.

<sup>57</sup> CA, *et al.* at 9 (emphasis added). *And see* CA, *et al.* discussing audit trails to track employee access, stating that “Carriers should be under a duty to record *all instances where a customer’s record is accessed*, who accessed the information, and for what purpose.” *Id.* at 12. While Qwest is cited as a major carrier that has a “similar system[ ] in place” (*id.*), Qwest is on record as stating that it does not have systems that track all instances of access to customer information. Nor do we believe such systems are required as a matter of reasonable business judgment. Qwest 2006 Comments at 12-13.

<sup>58</sup> *See, e.g.*, Qwest 2006 Comments at 10-13; Comments of National Cable & Telecommunications Association, CC Docket No. 96-115 and RM-11277, filed Apr. 28, 2006 at 5.

financial sector, there is no evidence that such features are necessary in the telecommunications sector with regard to CPNI.<sup>59</sup>

The Commission should reject pleas calling for particular carrier audit functionalities for all the reasons carriers and others previously articulated.<sup>60</sup> *CA, et al.* fails to prove that carriers currently have inadequate audit trails that threaten the prosecution of pretexters or others, or the management of employees.<sup>61</sup> Accordingly, the Commission should leave the matter of the design and implementation of appropriate audit trails generally to the carriers that must pay for, utilize, and keep them current.

Specific audit prescriptions should be confined to enforcement and remediation activities. The Commission should wait until circumstances raise concerns that a particular carrier is failing to take “reasonable means” to protect its customer information. Faced with such facts, the Commission is fully equipped to take appropriate enforcement action. Barring such facts, the Commission should defer to the reasoned judgment of management on this clearly commercial prerogative.

---

<sup>59</sup> *CA, et al.* at 9, where reference is made to a Wall Street Journal article about bank employees’ theft of information and the suggestion that an audit regime that has a high level of algorithms to detect unusual patterns might have caught the proposed theft. With unconstrained resources, businesses can achieve many things. The art is in managing the possible. *See* Qwest 2006 Comments at 13-16. *And see* Reply Comments of Verizon, filed June 2, 2006, CC Docket No. 96-115 and RM-11277 at 17-18.

<sup>60</sup> Alltel 2006 Comments at 5-6; BellSouth 2006 Comments at 18-22; Cingular Wireless LLC 2006 Comments at 22-23; Comptel 2006 Comments at 6-7; Qwest 2006 Comments at 13-16.

<sup>61</sup> Notwithstanding *CA, et al.*’s argument that the Commission should prescribe additional audit functionalities, *CA, et al.*’s narrative suggests the contrary, particularly with respect to pretexter attacks. *CA, et al.* references a limited number of situations where pretexters either attempted or successfully secured call-detail records of individuals. *CA, et al.* at 8. But *CA, et al.* does not argue, nor could it, that carrier audit trails were insufficient to address the matter in either civil or criminal fora. *See* Verizon Wireless 2006 Comments at 5-6; Cingular 2006 Comments at 2; Verizon 2006 Comments at 3.

**D. The Commission Should Not Prescribe Data Retention Or Destruction Timeframes Because Doing So Interferes With Reasonable Business Operations and Data Retention Programs.**

CA, *et al.* makes the unsupported, factual, statement that “[a] limitation on data retention enhances protection of CPNI.”<sup>62</sup> It does not say it “might” or “could” enhance such protection. It says that it does so. Some proof of its factual representation would have been nice.<sup>63</sup> CA, *et al.* could also have advanced the discussion had it addressed the already-filed record evidence opposed to EPIC’s previously-submitted data limitation proposal.<sup>64</sup> But it fails to do so. The combination is fatal to the effectiveness of CA, *et al.*’s arguments.

Equally problematic is the fact that CA, *et al.* proposes a data retention rule that lacks precision or pragmatism. Specifically, it proposes that “CPNI records . . . be deleted *immediately* after they are no longer needed for billing or dispute purposes.”<sup>65</sup>

---

<sup>62</sup> CA, *et al.* at 13.

<sup>63</sup> Once again, CA, *et al.* raises the spectre of identity theft with respect to data retention. *Id.* at 13. Qwest concedes that records that may contain social security numbers, that are accessed through a breach, might contribute to identity theft. This is true with respect to any business, not just telecommunications service providers. But as a general matter, we do not believe that telecommunications account or billing information is high stakes information in the realm of identity theft, and CA, *et al.* makes no attempt to prove that it is. The fact that a customer had activated call trace ten times in the last six months, or that a person subscribes to call waiting, is hardly information that would be useful in stealing the identity of another.

<sup>64</sup> EPIC Petition at 11-12. *And see* BellSouth 2006 Comments at 13-15; T-Mobile 2006 Comments at 16; Comments of US LEC Corp., CC Docket No. 96-115 and RM-11277, filed Apr. 28, 2006 at 5; Comments of Verizon Wireless, LLC, CC Docket No. 96-115 and RM-11277, filed Apr. 28, 2006 at 17-18. *Compare* NJ Rate Counsel at 4 (where it urges the Commission to obtain input from all stakeholders on the appropriate data collection and retention periods,” without acknowledging that facts and data on this matter are already part of the record).

<sup>65</sup> CA, *et al.* at 13. CA, *et al.* never defines “immediately,” a word that could have a wide range of interpretations. Does “immediately” mean “simultaneously?” “Within seconds?” “Within minutes?” Is “immediately” a matter of objective factual proof or something a carrier is permitted to determine? Does it really mean “within a reasonable amount of time?” Absent proof that retained data results in harm to consumers, is a mandate requiring destruction of data “immediately” arbitrary? Capricious?

Qwest and others have already addressed reasons why the Commission cannot restrict the purposes for which CPNI might be retained.<sup>66</sup> There are clearly legitimate business purposes and legal requirements for retaining data, including customer information, that go beyond “billing or dispute purposes.”<sup>67</sup> It is doubtful that the Commission’s jurisdiction would extend to *prohibiting* carriers from retaining records for tax or other legitimate business purposes. Nor would it be sage for the government to try to prescribe the reasonable scope of an identified “business purpose.”<sup>68</sup>

Another problem with CA, *et al.*’s proposed rule is that, like CA, *et al.*’s other proposals, it would pertain solely to telecommunications service providers, despite the fact that the “problem” CA, *et al.* identifies and proposes to solve is applicable to businesses in general. Yet a regulation such as the one proposed by CA, *et al.* would, to Qwest’s knowledge, be unique to Federal privacy regulation. Accordingly, absent a targeted data retention rule (such as the Commission has promulgated with regard to toll records),<sup>69</sup> the matter of data retention is best left to management judgment based on a particular business’s risk, revenue and litigation assessment.

---

<sup>66</sup> See, e.g., Qwest 2006 Comments at 16-18; BellSouth 2006 Comments at 31-32.

<sup>67</sup> Qwest 2006 Comments at 16-18.

<sup>68</sup> CA, *et al.* bemoans the fact that a carrier’s business purpose might encompass sharing CPNI with its business agents and partners in order to communicate with customers about products and services. CA, *et al.* at 13. Besides the fact that both types of communication are constitutionally protected, such use of customer information is routine in American business and hardly harmful or threatening to consumers.

<sup>69</sup> See 47 C.F.R. § 42.6.

**E. It Is Premature For The Commission To Prescribe “Information-Deletion” Functionalities For Mobile Phone Equipment, Since The Market Continues To Create And Offer Such Functionality.**

In the matter of data held in cell phones, like elsewhere, CA, *et al.* wants the government to intervene in the marketplace.<sup>70</sup> And, like elsewhere, it makes no persuasive argument that the marketplace is failing to respond to consumer privacy concerns or that current practices result in systemic or widespread privacy invasions. In fact, CA, *et al.* appears unknowledgeable about current cell phone information-deletion functionalities. As a result, it asks the Commission to require manufacturers to create functionalities that are currently commonplace -- *i.e.*, the ability of a consumer to delete personal information from the Menu Option of a cell phone.<sup>71</sup>

As Qwest noted in our opening comments, consumers generally have the ability to delete their personal information from a cell phone.<sup>72</sup> Given the readily-available self-help capabilities already designed and manufactured by carriers for their customers, the Commission has no reason to rush to action. Carriers should retain the business prerogative regarding the design, deployment and marketing of data deletion services.

Moreover, newer technology is creating additional capabilities regarding the deletion of information -- just as one would expect a responsive market to do. Newer smart phones are

---

<sup>70</sup> CA, *et al.* at 15 urges the Commission to act now to create carrier deletion rules for cell phone information.

<sup>71</sup> *Id.* at 19. *And see* NJ Rate Counsel at Section III. (recommending “that the rationale of the existing rules logically extend to . . . requiring mobile device manufacturers to provide consumers a means of insuring that their personal information can be efficiently deleted from mobile equipment”), Section VI. Presumably NJ Rate Counsel would be satisfied with the information put on the public record in the comment round indicating that such tools are currently available to consumers. The matter of whether consumers should be able to “transfer” CPNI (NJ Rate Counsel at Section VI.) from one mobile phone to another, and at what price, is beyond the scope of the current rulemaking; and, in any event, is already something that can be done under certain circumstances.

<sup>72</sup> Qwest Comments at 15-16.

being manufactured with capabilities for remote deletion, either by an individual or a network provider.<sup>73</sup> It is premature for the Commission to dictate how this technology or competitive choices are rolled out.

**F. CA, *Et Al* Fails To Demonstrate A Need For Its Other Proposed Government Mandates.**

CA, *et al.* seeks to insinuate comments into this *Further Notice* round that are either firmly resolved as a matter of law and regulatory policy, or that go beyond the scope of this *Further Notice* (sometimes themselves the subject of other pending *Further Notice* proceedings). For this reason alone, CA, *et al.*'s advocacy on these matters should be ignored.

First, CA, *et al.* urges the “adopt[ion] [of] a comprehensive opt-in policy.”<sup>74</sup> This despite the fact that: (1) **almost a decade ago** the Tenth Circuit Court of Appeals held that such a governmental policy violates the First Amendment rights of carriers and their customers;<sup>75</sup> (2) the Commission has concluded it cannot lawfully establish such a comprehensive policy;<sup>76</sup> and (3) the subject matter is outside the scope of the current *Further Notice* proceeding. It is odd that CA, *et al.* decides to address what it characterizes as the “economically preferable” arguments of CPNI opt-out proponents,<sup>77</sup> and that it admits that an opt-in regime “might

---

<sup>73</sup> It is this “smart phone” technology (*e.g.*, Blackberries that have phone functionality) that CA, *et al.* references with respect to Sprint’s “data kill” feature. *Id.* at 18. Other carriers and employers, as well, make use of this functionality.

<sup>74</sup> *Id.* at 10, 12, 22-24.

<sup>75</sup> See *US WEST v. FCC*, 182 F.3d at 1239.

<sup>76</sup> See *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; 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers’ Long Distance Carriers*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14874-75 ¶ 31, Separate Statement of Chairman Michael K. Powell at 14962 (2002).

<sup>77</sup> CA, *et al.* at 23.

decrease the amount of information in the marketplace,”<sup>78</sup> but ignores established law in this area that renders its proposal unlawful.

Second, CA, *et al.* leads off its comments with an argument speculating about the “serious and irreversible privacy problems for customers” that would attend “any sale of CPNI.”<sup>79</sup> But the *Further Notice* did not seek comment on this matter, and the issue of the sale of CPNI is the subject of another *Further Notice* proceeding.<sup>80</sup> If CA, *et al.* has a position on the matter of the sale of CPNI, it should file an *ex parte* in that still-pending proceeding.

Additionally, CA, *et al.*’s argument ignores the fact that Congress (rightly or wrongly, legally or not) has mandated that, in certain circumstances, aggregated CPNI be made available to others<sup>81</sup> (and certainly not for free, which means it might be sold). Furthermore, any blanket rule prohibiting the sale of CPNI would be an impermissible restriction on the alienation of property. (So too would a rule requiring “opt in” customer consent to such transfer, since the inability to secure such consents would essentially thwart the ability to sell.) And, finally, CA, *et al.* fails to show that carriers sell aggregated CPNI as a targeted source of revenue. Such an assertion has never been demonstrated and is counterintuitive, as the Tenth Circuit previously noted.<sup>82</sup>

---

<sup>78</sup> *Id.* at 24.

<sup>79</sup> *Id.* at 1, 22. *And see id.* at 14 (arguing that “forbidding [the] sale of CPNI based on aggregated data amounts to a lost source of revenue”).

<sup>80</sup> *See In the Matter of 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 Proprietary Network Information*, Notice of Proposed Rulemaking, 21 FCC Rcd 1782 (2006).

<sup>81</sup> 47 U.S.C. § 222(c)(3).

<sup>82</sup> *US WEST v. FCC*, 182 F.3d at 1237-38 (“While protecting against disclosure of sensitive and potentially embarrassing personal information may be important in the abstract, we have no indication of how it may occur in reality with respect to CPNI. Indeed, we do not even have indication that the disclosure might actually occur. The government presents no evidence regarding how and to whom carriers would disclose CPNI”; “Yet the government has not

### III. CONCLUSION

Qwest appreciates the Commission's continued dedication to the principles of consumer protection, including the protection of customer information. But in large part because carriers have already incorporated these concerns into their operations, as the marketplace and the statutory framework of the Act require them to do, further amendments to the CPNI rules are not necessary to accomplish that goal. Moreover, as many carriers argue, time is necessary to implement the Commission's most recent rule amendments. No new rules (and corresponding implementation deadlines) should be imposed on carriers at this time.

To the extent any of the harms speculated by commentators such as CA, *et al.* and NJ Rate Counsel actually arise, the Commission can proceed to address them through targeted enforcement action. Remediation mandates and their associated costs should be focused on situations where there is an identified need for such remediation. Such costs should not burden an entire industry and their customers, absent compelling evidence of the need for such burden. No such evidence has been presented to date.

Respectfully submitted,

QWEST COMMUNICATIONS  
INTERNATIONAL INC.

By: Kathryn Marie Krause  
Craig J. Brown  
Kathryn Marie Krause  
Suite 950  
607 14<sup>th</sup> Street, N.W.  
Washington, DC 20005  
303-383-6651  
Its Attorneys

August 7, 2007

---

explained how or why a carrier would disclose CPNI to outside parties, especially when the government claims CPNI is information that would give one firm a competitive advantage over another. This leaves us unsure exactly who would potentially receive the sensitive information.”)

CERTIFICATE OF SERVICE

I, Eileen Kraus, do hereby certify that I have caused the foregoing **REPLY**  
**COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC.** to be: 1) filed  
with the FCC via its Electronic Comment Filing System in CC Docket No. 96-115 and WC  
Docket No. 04-36; 2) served via e-mail on Ms. Janice Myles, Competition Policy Division,  
Wireline Competition Bureau at [janice.myles@fcc.gov](mailto:janice.myles@fcc.gov); 3) served via e-mail on the FCC's  
duplicating contractor Best Copy and Printing, Inc. at [fcc@bcpiweb.com](mailto:fcc@bcpiweb.com); and 4) served via First  
Class United States Mail, postage prepaid, on the parties listed on the attached service list.

/s/ Eileen Kraus

August 7, 2007

Davida Grant  
Gary Phillips  
Paul K. Mancini  
AT&T Inc.  
Suite 1000  
1120 20<sup>th</sup> Street, N.W.  
Washington, DC 20036

Karen Reidy  
Comptel  
Suite 400  
900 17<sup>th</sup> Street, N.W.  
Washington, DC 20006

Craig T. Smith  
Embarq  
5454 W. 110<sup>th</sup> Street  
Overland Park, KS 66211

David Bartlett  
Jeffrey S. Lanning  
Embarq  
Suite 820  
701 Pennsylvania Avenue, N.W.  
Washington, DC 20004

Kenneth F. Mason  
Frontier Communications  
180 South Clinton Avenue  
Rochester, NY 14646-0700

Kevin Saville  
Frontier Communications  
2378 Wilshire Boulevard  
Mound, MN 55364

Jan F. Reimers  
ICORE, Inc.  
326 S. 2<sup>nd</sup> Street  
Emmaus, PA 18049

John C. Pietila.....ITA  
Davis, Brown, Koehn, Shors & Roberts  
Suite 2500  
666 Walnut Street  
Des Moines, IA 50309-3993

Joshua Seidmann  
Independent Telephone and  
Telecommunications Alliance  
Suite 550  
975 F Street, N.W.  
Washington, DC 20004

Daniel L. Brenner  
Steven F. Morris  
National Cable &  
Telecommunications Association  
Suite 100  
25 Massachusetts Avenue, N.W.  
Washington, DC 20001-1431

Ronald K. Chen  
Kimberly K. Holmes  
Christopher J. White  
New Jersey Division of Rate Counsel  
11<sup>th</sup> Floor  
31 Clinton Street  
Newark, NJ 07171

Jill Canfield  
National Telecommunications  
Cooperative Association  
10<sup>th</sup> Floor  
4121 Wilson Boulevard  
Arlington, VA 22203

David L. Nace.....RCA  
Pamela L. Gist  
Lukas, Nace, Gutierrez & Sachs  
Suite 1500  
1650 Tysons Boulevard  
McLean, VA 22102

Jonathan Banks  
Indra Sehdev Chalk  
United States Telecom Association  
Suite 400  
607 14<sup>th</sup> Street, N.W.  
Washington, DC 20005

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

Stephen Seitz  
Vonage Holdings Corporation  
23 Main Street  
Holmdel, NJ 07733

Kenneth E. Hardman  
American Association of Paging Carriers  
Suite 250  
2154 Wisconsin Avenue, N.W.  
Washington, DC 20007-2280

Richard Metzger.....Comcast  
Lawler, Metzger, Milkman & Keeney  
Suite 802  
2001 K Street, N.W.  
Washington, DC 20006

Joseph W. Waz  
Brian A. Rankin  
Samuel F. Cullari  
Comcast  
1500 Market Street  
Philadelphia, PA 19102

James R. Coltharp  
Mary P. McManus  
Comcast  
Suite 500  
2001 Pennsylvania Avenue, N.W.  
Washington, DC 20006

Lynn R. Charytan.....MetroPCS  
Dileep S. Srihari  
Wilmer Cutler Pickering  
Hale and Dorr  
1875 Pennsylvania Avenue, N.W.  
Washington, DC 20006

Mark A. Stachiw  
Damien E. Falgoust  
MetroPCS Communications, Inc.  
Suite 800  
8144 Walnut Hill Lane  
Dallas, TX 75231

John J. Heitmann.....NuVox  
Jennifer M. Kashatus  
Kelley Drye & Warren  
Suite 400  
3050 K Street, N.W.  
Washington, DC 20007

Douglas G. Bonner.....Sprint Nextel  
Kathleen Greenan Ramsey  
Sonnenschein Nath & Rosenthal  
Suite 600, East Tower  
1301 K Street, N.W.  
Washington, DC 20005

Kent Y. Nakamura  
Frank P. Triveri  
Anthony M. Alessi  
Sprint Nextel Corporation  
2001 Edmund Halley Drive  
Reston, VA 20191

Matthew A. Brill.....Time Warner  
Stefanie R. Alfonso-Frank  
Suite 1000  
555 11<sup>th</sup> Street, N.W.  
Washington, DC 20004

Steven N. Teplitz  
Susan A. Mort  
Time Warner  
Suite 800  
800 Connecticut Avenue, N.W.  
Washington, DC 20006

Thomas J. Sugrue  
Kathleen O'Brien Ham  
Sara F. Leibman  
Shellie Blakeney  
T-Mobile USA, Inc.  
Suite 550  
401 9<sup>th</sup> Street, N.W.  
Washington, DC 20004

William F. Maher.....T-Mobile  
Joan E. Neal  
Morrison & Foerster  
2000 Pennsylvania Avenue, N.W.  
Washington, DC 20006-1888

Scott B. Tollefsen  
USA Mobility, Inc.  
6677 Richmond Highway  
Alexandria, VA 22306