

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

Implementation of the Telecommunications Act of 1996	)	CC Docket No. 96-115
	)	
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information	)	WC Docket No. 04-36
	)	
	)	

---

**REPLY COMMENTS OF AT&T INC.**

---

Davida Grant  
Gary Phillips  
Paul K. Mancini

AT&T Inc.  
1120 20<sup>th</sup> Street NW  
Suite 1000  
Washington, D.C. 20036  
(202) 457-3045 – phone  
(202) 457-3073 – facsimile

Its Attorneys

August 7, 2007

**TABLE OF CONTENTS**

	Page
I. INTRODUCTION AND SUMMARY .....	1
II. DISCUSSION .....	3
A. The Record Confirms that Additional CPNI Security Measures are Premature and Unwarranted .....	3
1. Mandatory Passwords .....	4
2. Physical Safeguards .....	5
3. Limiting Data Retention .....	6
B. The Commission Should Not Eliminate its Opt-out Regime .....	7
C. There is No Need for Regulations Requiring Carriers to Delete Customer Data Stored on Mobile Telephone Devices.....	11
III. CONCLUSION.....	13

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20054**

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	)	WC Docket No. 04-36
	)	

**REPLY COMMENTS OF AT&T INC.**

AT&T Inc. (“AT&T”), on behalf of its telecommunication affiliates, hereby files its reply comments in response to comments filed in the Further Notice of Proposed Rulemaking (“FNPRM”)<sup>1</sup> in the foregoing docket.

**I. INTRODUCTION AND SUMMARY**

The comments in this proceeding confirm the importance of protecting customer information from misuse or unauthorized access by fraudsters. All commenters – carriers, consumers, regulators and privacy groups – agree that the industry as a whole must be vigilant in safeguarding consumer records and working together to do so. In this regard, carrier commenters expressed that they are diligently working to implement the security measures recently adopted by the Commission to directly combat pretexting. Further, like AT&T, many commenters expressed that they are evaluating other mechanisms, beyond those required by the

---

<sup>1</sup> Implementation of the Telecommunications Act of 1996 et al., *Report and Order and Further Notice of Proposed Rulemaking*, CC Docket No. 96-115, WC Docket No. 04-36 (rel. Apr. 2, 2007)(“*2007 CPNI Order*”).

Commission, to further safeguard CPNI. Thus, the record clearly shows that carriers take their duty to protect CPNI from unscrupulous parties seriously.

As the record shows, Commission adoption of even more security measures at this juncture would be premature. Commenter after commenter explained that prudence dictates that the Commission afford the new measures, *which have yet to take effect*, an opportunity to work, before considering what, if any, additional measures are warranted.

Two commenters, the Electronic Privacy of Information Corporation (“EPIC”) and the Ratepayers Association, espouse a different view, however. The new rules, in their opinion, are insufficient to adequately protect customer information. They urged the Commission to adopt all of the measures proposed in the FNPRM. EPIC even went one step further and asked the Commission to eliminate its opt-out regime and require carriers to obtain opt-in approval before using or sharing CPNI for marketing purposes.

The measures proposed by EPIC and the Ratepayer Association would provide few, if any, benefits in the war against pretexting and any such benefits are far outweighed by their associated costs. Similarly, revisiting the opt-out regime is unnecessary because there simply is no correlation between opt-in or opt-out consent and pretexting, a fact EPIC has failed to refute.

Finally, as the record clearly shows, existing market-driven programs already exist to educate consumers regarding erasing data stored on their mobile devices. And carriers have, on their own, implemented measures to erase such data on refurbished equipment. Mandatory requirements in this context are therefore unwarranted.

## II. DISCUSSION

### A. The Record Confirms that Additional CPNI Security Measures are Premature and Unwarranted.

As many commenters have explained, the Commission's new CPNI rules will not take effect until December 2007.<sup>2</sup> Until those rules are implemented and given an opportunity to work, there is no reasoned basis for the Commission to further regulate the industry.<sup>3</sup> As AT&T explained, the Commission should first avail itself of the opportunity to review carrier reports regarding actions taken against databrokers and a summary of consumer complaints regarding unauthorized disclosures, as well as carrier notifications to the FBI of CPNI breaches before making any determinations whether additional rules are needed.<sup>4</sup>

Nevertheless, operating under the theory that more is always better, EPIC and the Ratepayers Association urge the Commission to adopt additional, specific CPNI measures, claiming that the new rules, while a step in the right direction, are inadequate to safeguard CPNI. This is a baseless assertion, given that the new rules have not even taken effect and neither of these commenters, nor the Commission, could reasonably conclude that the new rules are inadequate at this juncture. Moreover, as discussed below, these commenters make no credible effort to explain how their proposals would directly combat pretexting (if at all) and why the benefits of those proposals (if any) would outweigh the corresponding costs they will impose on consumers and the industry.

---

<sup>2</sup> See Comcast Corp. Comments at 1-2; COMPTTEL Comments at 1-2; Embarq Comments at 1-2; ICORE Companies Comments at 5; NCTA Comments at 2; NTCA Comments at 1; NUVOX Communications and XO Communications Comments at 2; Sprint Nextel Comments at 2; Time Warner Comments at 6; T-Mobile USA Comments at 2; USTelecom Comments at 2; USA Mobility Comments at 2; Vonage Holdings Corporation Comments at 2-3; Verizon Comments at 1.

<sup>3</sup> *Id.*

<sup>4</sup> See AT&T Comments at 3.

## 1. Mandatory Passwords

EPIC urges the Commission to require mandatory passwords for the release of *any* CPNI over the telephone, arguing that such regulation will ensure that only the customer accesses his or her account information.<sup>5</sup> The Commission, however, has already squarely rejected this argument with respect to call detail CPNI, finding that passwords, while an effective measure, could prove overly burdensome to both consumers and carriers.<sup>6</sup> This same logic applies with even more force to non-call detail CPNI, which is *less* sensitive from a customer privacy perspective.

As many commenters explained, their investigations have shown that pretexters, whether databrokers or disgruntled spouses or friends, want *calling records*.<sup>7</sup> They are not interested in a customer's total bill amount, the types of services a customer purchases or how many minutes of long distance service a customer has used – all routine requests involving non-call detail CPNI. Because consumers often forget their passwords,<sup>8</sup> a fact EPIC cannot refute, a mandatory password requirement for any type of CPNI will necessarily affect the ability of many consumers to expeditiously transact business on their account. Indeed, even EPIC concedes that consumers contact carriers “with simple requests that may not necessitate a password or the release of

---

<sup>5</sup> See EPIC Comments at 7.

<sup>6</sup> 2007 CPNI Order ¶¶16-19.

<sup>7</sup> See, e.g., Sprint Nextel Comments at 15-16; Verizon Comments at 2.

<sup>8</sup> See AT&T's Comments, filed April 28, 2006, wherein AT&T explains the results of the Ponemon Study. That study clearly shows that consumers dislike passwords because they tend to forget them. See also Verizon Comments at 5.

sensitive data.”<sup>9</sup> The Commission accordingly should refrain from mandating a password requirement for non-call detail information.

## **2. Physical Safeguards**

EPIC urges the Commission to require carriers to encrypt CPNI, arguing that this safeguard will protect CPNI from unscrupulous employees and data thieves.<sup>10</sup>

Most carriers, like AT&T, recognize that they have a duty to protect stored CPNI and have implemented procedures to physically safeguard that data.<sup>11</sup> Importantly, encryption is only one of many options that carriers employ. In addition to encryption, Comcast and Verizon, for example, transmit CPNI over secure, dedicated transmission channels.<sup>12</sup> Other carriers do not use encryption at all. Embarq, for example, generally does not transfer CPNI to third parties, but rather permits its agents to access its CPNI databases through secure logons.<sup>13</sup> To mandate a one-size-fits-all approach to physically safeguarding CPNI through encryption would therefore be costly, burdensome and unnecessary, particularly given the many effective options available for safeguarding CPNI. Notably, encryption of sensitive financial data is not mandated by the

---

<sup>9</sup> See EPIC Comments at 7.

<sup>10</sup> See EPIC Comments at 10. EPIC also urges the Commission to adopt audit trails. As a number of carriers explained, such a requirement would prove extremely costly and burdensome to implement with little utility in the war against pretexting. See Comcast Corp Comments at 6; Embarq Comments at 4; Comments of the Independent Telephone and Telecommunications Alliance at 3; Iowa Telecommunications Association Comments at 4; NUVOX Communications and XO Communications Comments at 5; Qwest Comments at 8-11; Sprint Nextel Comments at 10-13; Time Warner Comments at 9-10; USTelecom Comments at 4; USA Mobility Comments at 9-10. See also AT&T Comments, April 28, 2006.

<sup>11</sup> See Comcast Corp. Comments at 1-2; COMPTTEL Comments at 2-3; Embarq Comments at 4; NUVOX Communications and XO Communications Comments at 6-7; Sprint Nextel Comments at 13-14; T-Mobile USA Comments at 2; USTelecom Comments at 2; USA Mobility Comments at 2; Vonage Holdings Corporation Comments at 2-3; Verizon Comments at 1.

<sup>12</sup> See Comcast Corp Comments at 7-8; Verizon Comments at 15-17.

<sup>13</sup> See Embarq Comments at 4.

Gramm-Leach-Bliley Act, thus to require encryption of CPNI, which is arguably less sensitive, is unwarranted.

But perhaps the most compelling reason for not mandating such a requirement is that there is little evidence that third parties are hacking into carrier systems to obtain CPNI.<sup>14</sup> Indeed, EPIC tellingly offers nothing to substantiate its claim that existing carrier safeguards are inadequate to thwart hacking activities. The few examples cited by EPIC focus on pretexting and unauthorized access by dishonest employees. Not one references a breakdown in physical security measures, such as hacking.<sup>15</sup> Thus, any additional measure adopted should squarely focus on pretexting, not speculative concerns about hacking.

### **3. Limiting Data Retention**

EPIC claims that mandatory de-identification or deletion of CPNI after such data is no longer necessary for billing or dispute purposes is necessary because personally identifiable information, calling records and caller location are particularly vulnerable to misuse by identity thieves, stalkers and domestic abusers.<sup>16</sup> EPIC however fails to show that these unscrupulous parties have attempted to gain such information from *historical* CPNI.<sup>17</sup> The “sensitive” data cited by EPIC is equally available from current CPNI, which in AT&T’s experience, is the data targeted by third parties.<sup>18</sup> Thus, requiring carriers to eliminate or de-identify historical CPNI

---

<sup>14</sup>See, e.g. Embarq Comments at 4; Verizon Comments at 16.

<sup>15</sup> See EPIC Comments at 9-12.

<sup>16</sup> See EPIC Comments at 13.

<sup>17</sup> Historical CPNI is generally at least 6 months old and not generally stored in carrier databases. Often such information is archived or housed in databases not routinely accessed by representatives to handle customer inquiries.

<sup>18</sup> See also Sprint Nextel Comments at 15-16; Verizon Comments at 2.

will not alleviate or minimize the asserted harms. The myriad of additional security measures carriers must now implement however should.

Moreover, as the record confirms, there are many legitimate reasons for carrier retention of CPNI.<sup>19</sup> In addition to resolving billing and dispute issues, carriers need such data to develop new and better products and services for customers, for internal investigations, to assist customers in civil and criminal litigation, and to respond to non-billing related customer inquiries.<sup>20</sup> AT&T customers, for example, often ask for a historical breakdown of their services and associated charges when considering whether to move to a new pricing plan. Historical CPNI has also proven extremely useful to AT&T in its legal actions against pretexters and to law enforcement in investigations involving espionage, terrorism and other illegal activities. Carriers accordingly should continue to have the flexibility to retain CPNI as long as necessary for legitimate business uses

#### **B. The Commission Should Not Eliminate its Opt-out Regime**

In addition to the foregoing proposals, EPIC urges the Commission to eliminate its existing opt-out regime altogether and, instead, to require carriers to obtain opt-in consent prior to using or sharing such CPNI for marketing purposes.<sup>21</sup> As discussed below, EPIC's request is both legally suspect and unhelpful in combating pretexting.

In the *CPNI Order*, the Commission revised its CPNI consent rules to require carriers to obtain opt-in consent prior to sharing CPNI with independent contractors and joint venture

---

<sup>19</sup> See Sprint Nextel Comments at 15-20; Time Warner Comments at 7; Verizon Comments at 17-20.

<sup>20</sup> *Id.*

<sup>21</sup> See EPIC Comments at 22.

partners.<sup>22</sup> In that context, however, the Commission determined that it was in the public interest to do so because carriers purportedly lack sufficient control over these independent entities.<sup>23</sup> While AT&T disagrees with that conclusion, the Commission’s rationale for that conclusion does not apply to the use of CPNI by a carrier or its agents and EPIC’s arguments do not prove otherwise.<sup>24</sup>

Carriers can and are expected to exercise control over their agents – a fact recognized by the Commission. Indeed, the Commission previously concluded that it is appropriate to permit carriers to share CPNI with their agents on an opt-out basis because “the principles of agency law hold carriers responsible for the acts of their agents...thus [carriers] remain responsible for improper use or disclosure of consumers’ CPNI while in the hands of their agents.”<sup>25</sup> That reasoning continues to hold true today. Carriers exercise sufficient control over their agents, including those entities’ compliance with security measures. AT&T marketing agents, for example, must comply with AT&T’s authentication procedures prior to assisting customers with their inquiries<sup>26</sup> – a standard practice in the industry – and AT&T uses quality monitoring<sup>27</sup> to

---

<sup>22</sup> 2007 CPNI Order ¶37.

<sup>23</sup> 2007 CPNI Order ¶39.

<sup>24</sup> AT&T relies to a significant degree on its agents to provide marketing services. Needless to say, such arrangements and relationships are critical to the success of AT&T’s businesses.

<sup>25</sup> Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Proprietary Network Information and Other Consumer Information; Implementation of Non-Accounting Safeguards of Section 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*, CC Docket Nos. 96-115, 96-149, and 00-257, 17 FCC Rcd 14860 (2002) (*CPNI Third Report and Order*), ¶46.

<sup>26</sup> Like AT&T employees, these agents are required to comply with AT&T’s authentication requirements before permitting the caller to transact business on the account.

ensure compliance. Accordingly, extending the opt-in rules to carrier (and their agents') use of CPNI is unnecessary.

Moreover, requiring carriers to obtain opt-in consent prior to using or sharing CPNI for marketing purposes would not protect CPNI from pretexters. As AT&T demonstrated at length in its prior comments and reply comments in this proceeding,<sup>28</sup> which AT&T incorporates herein, there simply is no correlation between opt-in or opt-out consent and pretexting. A pretexter *pretends* to be the customer or its agent with the express goal of duping a customer service representative to gain access to the customer's CPNI. The customer's CPNI status for *marketing purposes* (opt-in or opt-out) simply has no relationship to how the customer's CPNI will be safeguarded in response to an inbound call from a pretexter to a customer service representative or in response to online requests. But even if there were such a correlation, the Commission could not curtail a carrier's commercial speech rights under the First Amendment based solely on that correlation.<sup>29</sup> Under the *Central Hudson* test,<sup>30</sup> the Commission is required to consider not only consumer privacy interests, but the burdens any governmental restriction would have on commercial speech. Weighing these factors, as AT&T and others have previously demonstrated, the Commission can only reasonably conclude that an opt-out regime is less burdensome on commercial speech and more narrowly tailored to advance the

---

<sup>27</sup> With quality monitoring, AT&T randomly observes calls between customers and employees/agents to confirm compliance, *inter alia*, with AT&T's authentication procedures.

<sup>28</sup> See generally AT&T Comments filed April 28, 2006; AT&T Reply Comments filed May 31, 2006.

<sup>29</sup> See AT&T Comments filed April 28, 2006 wherein AT&T details how an opt-in requirement would not satisfy the *Central Hudson* test.

<sup>30</sup> *Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n of N.Y.*, 447 U.S. 557 (1980).

government's interest than an opt-in regime.<sup>31</sup> Moreover, given the significant additional security requirements imposed under the new rules – which carriers and their agents must follow – there is no reasonable basis to conclude that carriers will be unable to sufficiently protect CPNI in instances where such data is shared with their marketing agents. Thus, EPIC's sweeping request to eliminate the opt-out regime is meritless.

As an alternative to an opt-in regime, EPIC asks that the Commission require carriers to inform customers of the identity of every affiliate, agent or entity to whom the customer's CPNI has been disclosed and to alert such customers anytime there is a change in the list of companies that receive their CPNI.<sup>32</sup>

Carriers are already required to notify customers of the entities to whom they provide CPNI, and must do so regularly where they rely on opt-out consent.<sup>33</sup> Notably, customers understand that carriers use agents to market on their behalf – every major industry does so. Customers also understand that affiliated companies use their data to provide them communications-related services. The total services approach is in fact based on such consumer expectations.<sup>34</sup> Customers that do not wish for their CPNI to be shared with carrier agents and affiliates for marketing purposes can and do restrict their CPNI. The Commission accordingly should not modify its CPNI notification requirement as EPIC proposes.

---

<sup>31</sup> See April 28, 2006 NPRM Comments filed by the following carriers: BellSouth at 27-32; Cingular at 13-14; CTIA at 12; Verizon at 22-26; Charter Communications at 14-21; Time Warner at 16-18.

<sup>32</sup> See EPIC Comments at 24.

<sup>33</sup> 47 CFR §64.2008(c)(2).

<sup>34</sup> *CPNI Third Report and Order*, ¶36.

**C. There is No Need for Regulations Requiring Carriers to Delete Customer Data Stored on Mobile Telephone Devices.**

The record confirms that the industry is already proactively taking steps to educate consumers regarding the need to erase data stored on their mobile devices prior to disposal or refurbishing.<sup>35</sup> Further, the record reflects that wireless carriers, without regulatory intervention, have implemented measures to erase data, or assist customers with erasing data stored on their mobile equipment before disposal or refurbishment of the device.<sup>36</sup> Sprint, for example, states that it has implemented various programs to remove customer data from mobile equipment.<sup>37</sup> T-Mobile states that the mobile devices used with its services generally allow customers to delete their data and that its representatives are available to assist customers with such deletion.<sup>38</sup> Further, T-Mobile's website provides customers information on how to erase their information prior to disposal.<sup>39</sup> Similarly, Embarq and Verizon Wireless have implemented processes to erase customer data on mobile equipment before reselling the devices.<sup>40</sup>

While these efforts are protecting customer's privacy interests, the Commission cannot reasonably expect carriers alone to guarantee the erasure of customer data. As a threshold matter, as the record explains, customers should, in the first instance, take steps to erase data from their equipment. While carriers are doing their part, as AT&T and Sprint explained,

---

<sup>35</sup> See Embarq Comments at 5; T-Mobile Comments at 8; Sprint Nextel Comments at 22-23.

<sup>36</sup> *Id.*

<sup>37</sup> See Sprint Nextel Comments at 22-23.

<sup>38</sup> See T-Mobile Comments at 8.

<sup>39</sup> *Id.*

<sup>40</sup> See Embarq Comments; *See also* [\(describing Verizon Wireless' recycling program\)](http://support.vzw.com/faqs/Company%20Information/faq_hopeline.html#item10).

“wiping” customer data is an intricate process that involves multiple parties, including carriers, manufacturers and technology developers.<sup>41</sup> For example, in many instances, carriers must rely on software provided by manufacturers to erase the data. Thus, making carriers responsible for ensuring that customer data is completely or permanently erased from handsets would not be reasonable.

Nor would it be appropriate to require carriers to offer customers remote deletion for lost or stolen equipment because that technology is simply not available for a large number of mobile devices in the industry. Feature phones, for example, have limited capabilities and generally use a simple web browser, which is not compatible with existing remote deletion software. Further, a number of smart mobile devices are built on closed operating systems which limit the ability of carriers to offer remote deletion solutions developed by third parties. AT&T is nevertheless working with device manufacturers to add security functions to their devices. The Open Mobile Alliance is examining industry standards to outline protocols and mechanisms needed for the storage, security and clearing of data on mobile devices. However, any such improvements or standards would be included in new devices and would not necessarily be compatible with all existing devices.

In any event, given that carriers already have processes in place for “wiping” data on handsets before reselling them, and are proactively educating consumers regarding the need to delete their data, regulatory intervention is not warranted. Carriers should continue to have the flexibility to work with manufacturers, vendors and consumers to institute the most appropriate refurbishment solutions.

---

<sup>41</sup> See AT&T Comments at 10-11; Sprint Comments at 23.

### III. CONCLUSION

For the foregoing reasons, the Commission should not adopt any additional CPNI security measures, should not revisit its opt-out regime, and should not require carriers to erase data stored on mobile devices.

Respectfully Submitted,

/s/ Davida Grant

Davida Grant  
Gary Phillips  
Paul K. Mancini

AT&T Inc.  
1120 20<sup>th</sup> Street NW  
Suite 1000  
Washington, D.C. 20036  
(202) 457-3045 – phone  
(202) 457-3073 – facsimile

August 7, 2007