



Anisa A. Latif
Associate Director
Federal Regulatory

AT&T Services, Inc.
1120 20th Street, N.W.
Suite 1000
Washington, D.C. 20036

202.457.3068 Phone
202.457.3071 Fax
al7161@att.com E-mail

July 19, 2007

Via Electronic Submission

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

**Re: ERRATUM
In the Matter of Implementation of the Telecommunications Act of 1996;
Telecommunications Carriers' Use of Customer Proprietary Network
Information and other Customer Information, CC Docket No. 96-115; IP
Enabled Services, WC Docket No. 04-36**

Dear Ms. Dortch:

On July 9, 2007, AT&T timely filed Comments in the above referenced proceeding. Due to an administrative error, the cover page and table of contents were omitted and the filing date was inadvertently deleted from the first page. Attached please find a corrected version of AT&T's Comments. Please substitute this corrected version in the record for the version filed on July 9, 2007. For your reference, the ECFS receipt of the original filing is also attached.

Thank you for your attention in this matter. Should you have any questions, feel free to contact me.

Sincerely,

/s/ Anisa A. Latif
Anisa A. Latif

Enclosure

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

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

COMMENTS OF AT&T INC.

David Grant
Gary Phillips
Paul K. Mancini

AT&T Inc.
1401 Eye Street, NW
Suite 1100
Washington, D.C. 20005
(202) 326-8903 – phone
(202) 408-8745 – facsimile

Its Attorneys

July 9, 2007

TABLE OF CONTENTS

| | Page |
|---|------|
| I. INTRODUCTION AND SUMMARY | 1 |
| II. DISCUSSION | 3 |
| A. Additional Commission action here would be premature | 3 |
| B. The Commission's two-prong approach was sufficient, rendering any additional mandatory CPNI measures unnecessary | 4 |
| C. The Commission should not impose new regulations on carriers to erase information stored on mobile communications devices | 9 |
| III. CONCLUSION | 12 |

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

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

COMMENTS OF AT&T INC.

AT&T Inc. ("AT&T"), on behalf of its affiliates, respectfully files these comments in response to the Commission's Further Notice of Proposed Rulemaking ("FNPRM")¹ in the above-captioned docket on the use of customer proprietary network information ("CPNI").

I. INTRODUCTION AND SUMMARY

In the April 2007 *CPNI Order*, the Commission concluded that its existing CPNI regulations were inadequate to protect CPNI from pretexters, and adopted extensive additional CPNI measures requiring carriers to further secure CPNI, including authentication, password and notification requirements. Additionally, the Commission committed to vigorously enforce the CPNI rules and take action against carriers that do not take sufficient steps to protect CPNI.² The Commission now asks whether it should adopt even more requirements to combat pretexting. Further, the Commission asks

¹ Implementation of the Telecommunications Act of 1996 et al., *Report and Order and Further Notice of Proposed Rulemaking*, CC Docket No. 96-115, RM-11277 (rel. April 2, 2007) ("*CPNI Order*").

² *Id.*, ¶ 63.

whether it should mandate that carriers take additional actions to protect customer information stored on mobile communication devices.

AT&T shares the Commission's concerns in protecting customer information from pretexters and other unscrupulous parties. In today's intensely and increasingly competitive environment, carriers must appropriately protect their customers' information if they are to succeed in the marketplace. Accordingly, AT&T has strong incentives to take all necessary steps to safeguard CPNI, and continues to proactively do so.

While AT&T supports the Commission's efforts to thwart pretexters from improperly accessing CPNI, we believe that the imposition of additional regulatory mandates is premature at this time. The extensive new CPNI requirements adopted by the Commission are more than sufficient to protect consumers from pretexters. Moreover, the Commission's new CPNI requirements, which were just adopted in April, will not even become effective for at least another five months. Carriers should be afforded a reasonable opportunity to implement *those* requirements before any new requirements are considered. The Commission also should carefully evaluate the efficacy of those requirements, and their burdens on consumers, before making any determination as to whether other measures are warranted. Indeed, in the absence of any record indicating that further measures are warranted, imposing additional regulation here will only burden consumers and eliminate the flexibility carriers need to best protect their customers' sensitive information.

Finally, given that removing customer data stored on mobile devices during the refurbishment process is a complex undertaking that often requires coordinated efforts by carriers, handset manufacturers and third-party vendors of refurbishment services, the Commission should not impose strict new rules that dictate the manner in which customer data is removed from mobile devices when they are refurbished. Instead, the Commission should encourage all of the relevant parties in the refurbishment process to follow industry best practices, which enable mobile devices to be refurbished in a cost-effective fashion that serves the interests of the price-sensitive consumers who are the ultimate beneficiaries of refurbished handsets.

II. DISCUSSION

A. Additional Commission action here would be premature.

Although AT&T supports the Commission's efforts to curtail pretexting, we encourage the Commission to let carriers have a reasonable period of time to implement the new CPNI rules before taking up the question of whether further CPNI requirements are necessary. The new CPNI rules are not even in effect yet, and will not be in effect for at least another five months. The Commission could not meaningfully examine the impact of the new rules on pretexting – or the possible burdens *those* rules may have on consumers or carriers – until the new requirements have been fully implemented and given an opportunity to work. Importantly, the new rules require carriers to file reports on actions taken against data brokers and consumer complaints regarding unauthorized access to CPNI. Such information should be carefully evaluated by the Commission in assessing the efficacy of the new rules. Only after a thorough examination of that

information – together with a prudent assessment of the burdens imposed on consumers – should the Commission consider whether additional measures to protect CPNI are warranted.

B. The Commission’s two-prong approach was sufficient, rendering any additional mandatory CPNI measures unnecessary.

In the *CPNI Order*, the Commission took a two-pronged approach to further protect CPNI from improper disclosure, the first of which requires carriers to implement an array of CPNI security requirements.³ Second, the Commission committed to vigorously enforce the CPNI rules and stressed its expectation that carriers will implement additional measures, beyond the minimum requirements adopted by the Commission.⁴ While all carriers must adhere to certain minimum security requirements, the Commission reasoned that its two-pronged approach properly balanced consumer privacy interests with carrier burdens because carriers would retain the flexibility and incentive to proactively adopt security measures most appropriate to their business and customers.⁵

³ The measures include authentication requirements for the release of call detail information over the telephone, mandatory password requirements for online account access, customer notification of significant account changes, and customer and law enforcement notification of unauthorized disclosures of CPNI. These measures, the Commission reasoned, would directly target pretexting by minimizing the opportunity for pretexters to gain access to arguably the most sensitive customer information; alerting consumers to possible unauthorized disclosures so that they can take all necessary steps to safeguard their information; and providing law enforcement the information it needs to initiate enforcement-related actions. *Id.*, ¶¶ 13-33.

⁴ *Id.*, ¶65.

⁵ In reaching this conclusion, the Commission reasoned that its approach would: (1) allow carriers to implement whatever security measures are warranted in light of their technological choices, (2) create a diversity of security practices that will enable market forces to improve carriers’ security measures over time, (3) avoid creating unnecessary regulatory barriers that could impede carriers

Notably, the Commission highlighted certain requirements as appropriate additional measures carriers could implement to protect CPNI – measures for which it seeks additional comment in the *FNPRM* – but expressly declined to mandate these requirements, instead leaving it to carriers to determine if such measures are warranted.⁶ To now mandate specific additional CPNI measures, namely passwords for non-call detail information, audit trails, physical safeguards of CPNI and/or data retention limitations, would circumvent the careful reasoning and analysis underlying the two-prong approach.

First, and perhaps most significantly, certain of these requirements could impose substantial burdens on consumers without any commensurate benefits. As AT&T has previously detailed in this docket, study after study has shown that customers do not like to use passwords and those who do often forget them, rendering them ineffective as a regulatory tool.⁷ And with respect to non-call detail information, the associated consumer burdens are even more pronounced. Based on AT&T's experience, pretexters want to know who customers call, not information regarding the types of services they purchase, or information regarding their service troubles or bill amount. Further restricting the ability of customers to obtain such non-call-related CPNI would unduly burden customers without providing any significant deterrent to pretexting.

from adapting to new threats as the methods used by data brokers evolve, and (4) alleviate commenters' concerns that specific safeguard rules could provide pretexters with a "roadmap" of how to obtain CPNI without authorization. *Id.*, ¶ 65.

⁶ *Id.*, ¶ 64.

⁷ See Comments of AT&T, filed April 28, 2007.

Second, imposing additional rules here would limit carrier flexibility to the detriment of consumers. At the same time it adopted new carrier security procedures for CPNI, the Commission recognized that carriers' should have the ability to implement those security mechanisms best suited for their individual circumstances.⁸ Without question, the Commission considered some degree of carrier flexibility to be a critical part of its overall approach to safeguarding CPNI. In touting its two-prong approach, the Commission, for example, stated that the approach would allow carriers to "implement *whatever* security measures are warranted in light of their technological choices," and further would ensure a high a level CPNI protection "because carriers w[ould] have sufficient incentive and ability to adopt *whatever* security mechanisms work best with their existing systems and procedures."⁹ (emphasis added) Additional action here by the Commission would virtually nullify the expertise carriers have gained in protecting the security of their customer information and could have the unintended consequence of eviscerating the diversity of CPNI security procedures adopted in the industry, results neither intended by the two-prong approach nor consistent with the public interest.

The potentially adverse impact such Commission action would have on carrier security practices is not theoretical. For example, consistent with the *CPNI Order*, AT&T has chosen not to require passwords for telephone authentication because most customers either do not want them or often forget them. A mandatory password requirement as proposed in the *Notice* would therefore unnecessarily burden AT&T – as well as its

⁸ 2007 *CPNI Order*, ¶165.

⁹ *Id.*

customers – and prevent us from more effectively using our resources to implement authentication mechanisms better suited to our clientele.

Similarly, there are a number of ways that carriers can physically safeguard CPNI using the flexibility afforded by the *CPNI Order*. AT&T for example uses encryption in many instances to protect the transfer of CPNI to third parties and requires employees, agents, vendors and other parties to adhere to certain security procedures prior to gaining access to AT&T's CPNI databases. AT&T however recognizes that there are other equally viable methods to physically safeguard CPNI. A one-size-fits all approach, as suggested by the *Notice*, would limit a carrier's ability to choose the most effective and efficient physical safeguards, given its existing technology choices, systems and customer needs.

Third, mandating additional CPNI requirements and eliminating the flexibility afforded by the *CPNI Order* could discourage carriers from proactively developing innovative methods to combat pretexting. Compliance with the *existing* CPNI regulatory requirements is expensive, and time, labor, and resource intensive. When choosing to allocate resources, carriers will devote the lion's share to compliance with existing CPNI regulatory mandates, which necessarily will impact their ability to proactively pursue other innovative solutions for CPNI security. Additional regulations that eliminate the flexibility the Commission gave carriers to combat pretexting in the *CPNI Order* could have adverse consequences in the long run because they would force carriers to pursue reactive, one-size-fits-all Commission-mandated solutions rather than developing proactive, new technologies and practices to safeguard consumer privacy.

Finally, the specific requirements proposed in the *FNPRM* would be of little utility in the war against pretexting, and any minimal benefits to be gained would be far outweighed by the associated costs. As already explained, requiring mandatory passwords for non-call-detail CPNI will not thwart pretexting because pretexters seek out call detail information. Audit trails, while useful mechanisms to monitor employee access to CPNI, are of little value in ferreting out a pretexter because they only show that an employee accessed a customer's account at the behest of a person claiming to be the customer. Similarly, the destruction or de-identification of CPNI after a period of time would be of little value because *dated* information has minimal, if any, benefit to pretexters. In AT&T's experience, these unscrupulous parties want to know who customers are calling now, not a year or two ago. Further, as AT&T detailed in its prior comments, such a requirement could have the unintended consequence of adversely impacting a carrier's ability to respond to its customers needs, and respond to law enforcement inquiries.¹⁰

Given these concerns, the Commission should refrain from adopting additional CPNI measures. Rather, it should adhere to the two-pronged approach articulated in the *CPNI Order*, which requires carriers to implement certain CPNI protections, but affords them the necessary flexibility to determine what additional CPNI measures are most appropriate, effective and efficient to secure CPNI. And where a carrier fails to take sufficient action to safeguard CPNI, the Commission can take enforcement action, as it has committed to do.

¹⁰ *Id.* at 16-17.

C. The Commission should not impose new regulations on carriers to erase information stored on mobile communications devices.

In addition to the preceding CPNI measures, the Commission asks whether it should adopt regulations to protect customer information stored on mobile communications devices in the context of requiring carriers to “eras[e] customer information on mobile equipment prior to refurbishing the equipment.”¹¹ Although AT&T proactively takes a variety of steps to erase customer information on mobile devices that are refurbished for sale through our stores, we believe that the adoption of rules mandating particular erasure requirements are both unwarranted and potentially counterproductive.

As an initial matter, decisions about what personal data to store, or not to store, on a mobile device rest with the consumer. Carriers do not typically have access to such information and play no role in determining what information a consumer chooses to store on mobile devices or how that information is used. Indeed, in some respects, mobile communications devices are becoming more like computers, laptops, personal digital assistants and other devices that permit customers to store their information. In the same vein that consumers erase information stored on those devices, (or shred paper copies of bills or other documents that contain personal information), consumers are necessarily in the best position to know what data they have stored on their mobile devices and to take responsibility for safeguarding and erasing that information before disposal or recycling the device.

¹¹ *Id.*, ¶ 72.

Even so, AT&T has, as part of its overall consumer privacy policies, proactively implemented measures to erase customer information stored on mobile equipment that will be refurbished and sold by AT&T. Specifically, AT&T sends mobile devices to a third-party vendor that specializes in refurbishment. This vendor uses the equipment manufacturer's software in the device to set the mobile equipment back to the factory settings, which has the effect of erasing or "wiping" all customer information stored on the equipment. AT&T relies on a vendor to perform these specialized functions because AT&T does not manufacture mobile devices and has no control over the functionality embedded in mobile equipment for the removal of stored information. While AT&T has implemented processes to wipe customer information from equipment that will be refurbished, AT&T and its vendor wholly rely on the manufacturer's software to erase such data.¹² AT&T also requires the vendor to audit its performance to assure that it is wiping all personal data. Further, AT&T monitors the practices in its retail stores to ensure that returned phones are sent to the vendor for wiping, rather than having AT&T employees perform such tasks

In addition to instituting these refurbishment procedures, AT&T, along with the wireless industry, has taken measures to raise consumer awareness about recycling and reuse of mobile devices, including the deletion of personal data stored on such devices. AT&T, for example, provides consumers instructions regarding the recycling of mobile devices on its Reuse and Recycle website and refers customers to the manufacturer's

¹² For this reason alone, the Commission could not practicably impose a mobile device erasure requirement solely on carriers.

instructions for deleting personal information.¹³ CTIA and its member companies have designed and launched a comprehensive national recycling program, Wireless...The New Recyclable™, which provides consumers comprehensive information about recycling mobile devices.¹⁴ In particular, the program's website provides information on the steps consumers should take prior to recycling, including erasing personal information, as well as a link to the "Cell Phone Data Eraser" tool, which provides consumers easy access to various device manufacturer instructions for removing stored information.¹⁵

Given the extensive measures that AT&T already employs to erase customer information from mobile devices during the refurbishment process, there is simply no need for the Commission to adopt rules mandating such practices. Moreover, because of the numerous parties involved in the refurbishment process (carriers, equipment manufacturers, refurbishment vendors and consumers), carriers like AT&T must have maximum flexibility to work with those parties to institute cost-effective refurbishment solutions that safeguard customer privacy while enabling AT&T to offer affordable refurbished handsets to price-sensitive consumers. Any one-size-fits-all erasure mandate that would limit such flexibility and impose additional burdens on AT&T would ultimately harm those consumers by increasing the prices they pay for refurbished mobile devices.

¹³ See <http://www.wireless.att.com/about/community-support/recycling.jsp>.

¹⁴ See <http://www.recyclewirelessphones.com>.

¹⁵ See http://www.wirelessrecycling.com/home/data_eraser/.

III. CONCLUSION

For the foregoing reasons, the Commission should not adopt any additional CPNI security measures, or 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 20th Street NW
Suite 1000
Washington, D.C. 20036
(202) 457-3045 – phone
(202) 457-3073 – facsimile

July 9, 2007



Federal Communications Commission

The FCC Acknowledges Receipt of Comments From ...

AT&T Inc.

...and Thank You for Your Comments

Your Confirmation Number is: **200779716252**

| | |
|---------------------------------|-----------------------|
| Date Received: | Jul 9 2007 |
| Docket: | 96-115 |
| Number of Files Transmitted: | 1 |

DISCLOSURE

This confirmation verifies that ECFS has received and accepted your filing. However, your filing will be rejected by ECFS if it contains macros, passwords, redlining, read-only formatting, a virus or automated links to source documents that is not included with your filing.

Filers are encouraged to retrieve and view their filing within 24 hours of receipt of this confirmation. For any problems contact the Help Desk at 202-418-0193.

[Initiate a Submission](#) | [Search ECFS](#) | [Return to ECFS Home Page](#)

[FCC Home Page](#)

[Search](#)

[Commissioners](#)

[Bureaus/Offices](#)

[Finding Info](#)

updated 12/11/03