

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

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information)	
)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	

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

April 28, 2006

TABLE OF CONTENTS

	Page
INTRODUCTION AND SUMMARY	1
I. NATURE AND SCOPE OF UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION	4
II. ADDITIONAL MEASURES TO PROTECT CUSTOMERS.....	6
A. Authentication.....	7
1. Passwords.....	8
2. Customer Notification.....	11
B. Other Measures	14
III. APPLICABILITY TO VOIP PROVIDERS.....	19
CONCLUSION	22

**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)	
)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	

COMMENTS OF AT&T INC.

AT&T Inc. ("AT&T"), on behalf of its telephone companies, hereby files these comments in response to the Notice of Proposed Rulemaking ("NPRM")¹ in the foregoing docket.

INTRODUCTION AND SUMMARY

AT&T supports the Commission's decision to open this proceeding to examine allegations regarding the widespread misappropriation of customer proprietary network information ("CPNI"), and in particular claims that data brokers, private investigators and others routinely have obtained unauthorized access to personal telephone records – such as call detail records and unpublished telephone numbers – and offered to sell such information. In the past several months, as evidence of some of these unscrupulous actors' actions have come to light,

¹ Implementation of the Telecommunications Act of 1996 et al., *Notice of Proposed Rulemaking*, CC Docket No. 96-115 RM-11277 (rel. Feb. 14, 2006).

the Commission understandably has become concerned about the security of consumers' private information, and the sufficiency of carrier practices and procedures to maintain the confidentiality of personal telephone records. This proceeding provides an opportunity for the Commission to explore these allegations, determine the nature and scope of any unauthorized access to CPNI, determine if any measures are warranted to prevent such access in the future, and provide consumers additional assurance that their private information will remain confidential.

To the extent the Commission determines that regulatory intervention in this area is warranted, it should ensure that any measures or standards it adopts meet certain basic principles. First, any standards or measures the Commission adopts must carefully balance consumers' privacy concerns with the costs and burdens that such measures would impose on consumers and carriers alike, as well as the legitimate business needs of carriers. Overly burdensome or excessively elaborate security measures could create more problems than they solve. Consumers may need access to their personal telephone records for a variety of reasons – such as resolving billing issues, verifying customer account information, and monitoring their children's use of the telephone, among other things. Heightened restrictions on access to such information could make it more difficult for them to do so. Mandatory passwords, in particular, may be problematic for many consumers and not consistently effective because they are so often forgotten.

Second, the Commission should recognize that protecting consumer privacy will require carriers, customers, lawmakers and law enforcement officials to work in tandem to guard against unauthorized access to CPNI. To be sure, carriers must take reasonable steps to safeguard CPNI from third parties. But customers too must proactively guard their information and ensure that

they do not inadvertently give third parties information that would allow them to obtain easy access to their CPNI. By the same token, lawmakers and regulators must enact tougher rules to establish meaningful penalties for persons or entities that fraudulently access customer information and law enforcement must vigorously enforce such laws. Simply placing the responsibility of protecting customer information solely or primarily on the shoulders of telecommunications carriers would be neither effective nor appropriate.

Third, it should go without saying that the Commission should ensure that any measures it adopts in this proceeding are narrowly tailored and impose no greater burdens or restrictions than are reasonably necessary to address a demonstrated problem. For example, AT&T is aware of no evidence that hackers have been able to access CPNI, and proposals to require carriers to encrypt CPNI thus are unnecessary and unwarranted.²

Applying these principles, the Commission reasonably could establish customer authentication rules prescribing certain minimum standards or procedures regarding the means by which carriers must verify a customer's identity before disclosing that customer's CPNI. While mandatory passwords are unnecessarily burdensome and authentication procedures that rely solely on a customer's name, address and/or phone number may be insufficient because they rely on readily available public information, the Commission reasonably could conclude that all carriers should authenticate a customer's identity using non-public information prior to releasing CPNI over the telephone or online. Such a requirement would directly address the purported problem at issue here – pretexting – without unduly taxing carriers' resources or unnecessarily

² Likewise, as discussed below, modifying the existing opt-out rules is unnecessary. Further, there is no reason to require carriers routinely to submit to the Commission a summary or other report regarding all actions taken against data brokers or of all consumer complaints because the Commission retains full authority to require carriers to provide such information in the context of an investigation, and requiring carriers to routinely file such reports could provide fraudsters a roadmap to circumvent carriers' methods and procedures to safeguard CPNI.

burdening consumers. The Commission could reasonably conclude that carriers should maintain audit trails to facilitate investigations of possible unauthorized access by carrier employees. Likewise, the Commission could reasonably conclude that carriers should notify customers of the release of their CPNI in instances where the carrier determines a pretexter, hacker or other unauthorized third party was involved. Finally, the Commission might reasonably conclude that requiring carriers to file their annual CPNI certifications would assist the Commission in ensuring compliance with its CPNI rules.

I. NATURE AND SCOPE OF UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION

In the NPRM, the Commission solicits comment on EPIC's allegations that unauthorized third parties have exploited loop holes in carriers' existing CPNI safeguards to access private telephone information through pretexting, hacking and possibly through dishonest carrier employees. In particular, the Commission seeks comment on the nature and scope of the problems identified by EPIC,³ as well as information concerning the methods and procedures carriers currently use to maintain and secure CPNI, and whether and how data brokers and other unauthorized third parties have circumvented those procedures to obtain CPNI.⁴

AT&T has devoted significant resources, and implemented a variety of practices and procedures, to safeguard the privacy of its customers' private telephone information. As an initial matter, to prevent employee misuse or improper disclosure of CPNI, AT&T generally limits access to CPNI only to those employees who need such access to perform their job functions, and trains these employees on the proper use and protection of CPNI. To protect the security of its servers and the information contained therein, in most cases AT&T requires

³ NPRM ¶11.

⁴ *Id.*

employees and customers to provide user names and passwords to access sensitive data, and uses industry standard encryption methods to protect data transmissions. In addition, to thwart unauthorized access to CPNI by third parties, AT&T requires its customer service representatives to verify the identity of its customers using personal or account data (or, at the customer's request, a password) prior to releasing account information over the telephone, and requires customers, after initial setup, to provide a password before they can access their account information online. Additionally, AT&T assists customers in reporting any fraudulent activity to law enforcement officials, and works closely with law enforcement in any investigation of alleged fraud or other criminal conduct.

More generally, AT&T has in place a Code of Business Conduct ("Code") applicable to all employees, which requires them to safeguard the privacy of customer communications and records. Any employee who fails to meet any of the standards set forth therein is subject to disciplinary action, up to and including dismissal. AT&T also investigates any allegation that an employee(s) has breached the Code and, where appropriate, takes disciplinary action and initiates corrective action to prevent future recurrences. AT&T further has charged several internal organizations with protecting its servers, systems, customer communications and records, and investigating security breaches to ensure the integrity of AT&T's network and processes. Notably, AT&T has a Privacy organization to ensure the privacy of customer information.

Based on a review of year 2005 internal investigations of alleged unauthorized third party access to customer records, AT&T has identified only a *de minimis* number of cases in which a customer or employee alleged that such unauthorized access may have occurred.⁵ And, upon close examination, AT&T has determined that almost half of those cases did not entail any

⁵ In light of the heightened attention to the privacy of customer records, AT&T has initiated internal investigations to determine if pretexters can access its wireline records.

unauthorized access to CPNI. Even then, in most instances, the party obtaining unauthorized access was an employee or other individual with a personal relationship with the affected customer, such as a family member, friend or acquaintance. It is therefore not apparent to AT&T that unauthorized access to customer information by AT&T employees is rampant. AT&T has yet to uncover any evidence of hacking.

II. ADDITIONAL MEASURES TO PROTECT CUSTOMERS

As discussed above, before the Commission mandates any additional CPNI safeguards, it must carefully evaluate whether the potential benefits of any such requirements outweigh the significant costs that stringent restrictions on customer access to CPNI would impose on customers and carriers alike. AT&T recognizes that EPIC has identified certain entities that claim to be able to obtain CPNI with impunity. However, on balance, AT&T believes that the restrictions and safeguards proposed by EPIC go too far and are not narrowly tailored to address the purported harms.

That said, the law imposes on all telecommunications carriers a duty to protect the confidentiality of customer proprietary information, and it would not be unreasonable for the Commission to impose certain duties in that regard, even absent evidence of rampant fraud. In particular, as discussed below, the Commission could establish certain minimum authentication standards or procedures for verifying a customer's identity before providing access to that customer's CPNI. The Commission also could reasonably require carriers to maintain audit trails to facilitate investigations of alleged breaches of customer confidentiality, to notify customers of the release of their CPNI where fraudulent access by a third party occurred, and to file with the Commission annual CPNI compliance certifications.

A. Authentication

As noted above, AT&T already has established methods and procedures to authenticate a customer's identity prior to releasing that customer's CPNI over the telephone or online. But, while those procedures appear to have largely succeeded in preventing unauthorized access to its customer information thus far, AT&T recognizes that the Commission could reasonably conclude – even in the absence of evidence of “rampant” pretexting – that certain minimum authentication measures are necessary and appropriate to ensure that all carriers have adequate procedures to safeguard CPNI. In particular, consistent with the principles previously outlined, the Commission reasonably could require that all carriers verify customer identity using non-public information prior to releasing CPNI over the telephone or online. Such a requirement would directly address the issue of pretexting, which is the catalyst for this proceeding, without imposing undue burdens on consumers and unnecessary costs on carriers.⁶ Such a requirement also would ensure that all carriers take reasonable and appropriate steps to protect the proprietary information of their customers, consistent with the requirements of Section 222(a), while affording carriers flexibility to implement authentication methods best suited to their particular customer and business needs.⁷

⁶ Insofar as many, if not most, legitimate businesses require customers to provide some customer identification or information (albeit information that may be readily available to the public through, *inter alia*, telephone directories, such as name, address and/or phone number) to access private records, requiring carriers to verify a customer's identity based on non-public information would impose little additional costs, but would be more effective in safeguarding customer information from unauthorized access.

⁷ AT&T would favor a safe harbor for carriers that implement the foregoing requirements, as it appropriately recognizes that carriers, no matter the authentication method, cannot prevent all fraudulent access to CPNI. In this regard, AT&T proposes that carriers be required to demonstrate that they have established adequate written methods and procedures for authenticating customer identity, as described above, have adequately trained their personnel in such procedures, have audit trails in place to detect unauthorized employee access to customer accounts, and have disciplinary measures in place should employees fail to comply with those requirements.

On the other hand, other authentication measures proposed by EPIC are not only unnecessary but would so encumber consumer access to CPNI as to be contrary to the interests of consumers. The use of passwords and PINs in today's electronic age is so proliferated that consumers frequently forget their passwords or, to avoid forgetting, choose a password that a pretexter could readily guess. Mandatory password authentication procedures could thus be burdensome for consumers, burdensome for carriers, and not particularly effective. Similarly, proposals to require notice to customers before or after disclosing their CPNI would annoy customers and impose burdens that outweigh any conceivable benefits.

1. Passwords

Since consumers would be the intended beneficiaries of any authentication requirements imposed by the Commission, it is particularly telling that most consumers prefer not to use passwords to access their customer account and other private information. In a recent study on passwords and identity verification conducted by the Ponemon Institute,⁸ when asked whether companies should require customers to provide a unique password to access private information, the vast majority of respondents – fully 87% – opposed the use of passwords.⁹ When asked to choose the top two reasons for opposing mandatory passwords, 63% of respondents¹⁰ stated that “[i]t is inconvenient for me to remember passwords,” and 60% stated that “[p]asswords are not necessary if the company has other ways of determining who I am.”¹¹ Further, when asked to

⁸ 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) (“Ponemon Study”)

⁹ *Id.* at 340.

¹⁰ The respondents here initially answered that they opposed having to provide a password after the company had already verified their identity from personal data.

¹¹ Ponemon Study at 337.

choose between the following three authentication options, (1) password or three pieces of personal data, (2) mandatory passwords, or (3) mandatory three pieces of data, two-thirds of the respondents stated that they preferred option 1.¹² Only 13% selected option 2, mandatory passwords. These results are consistent with AT&T's own experience that customers seldom request password protection for their accounts.

Even those customers who choose to password-protect their accounts may, and often do, experience delays and other problems accessing their customer account information because they forget the password they selected. Given that AT&T's customers contact AT&T regarding their accounts relatively infrequently (residential customers, for example, contact AT&T only four times per year, on average), it is not surprising that they often have difficulty remembering their passwords. Again, AT&T's experience is consistent with the results of the Ponemon Study, which found that 88% of respondents had forgotten a password or PIN at least once in the previous two years and had to reset it.¹³

When AT&T's customers forget their passwords, they generally expect that AT&T will employ other methods to confirm their identity, such as by asking them to provide one or more pieces of customer-specific data. But, presumably, if the Commission were to impose a mandatory password requirement, it would prohibit carriers from using alternative means to authenticate customer identity – otherwise there would be no need for mandatory passwords. In that case, a customer who forgot her password would be required to wait until her password was reset, and a temporary password was sent to her e-mail address (or via mail to her billing address if the customer did not have Internet access). Either way, customers are inconvenienced, often

¹² *Id.* at 341.

¹³ *Id.* at 339.

severely, and, in some cases, they are denied access to their account information for a considerable period of time. It would be a serious mistake for the Commission to subject consumers to such burdens absent a compelling need and no adequate alternative.

Here there is no compelling need, not only because it is not clear that pretexting actually is a “rampant” problem, but also because requiring mandatory passwords is not likely to be any more effective than other authentication requirements. As the Ponemon Study results, discussed above, show, many consumers forget their passwords, and many others rely on insecure methods to recall their passwords for fear that they will forget them. A recent British survey entitled, “How Consumers Remember Passwords,”¹⁴ further confirms the point. That survey showed that many Internet users, especially older users, write down their passwords to remember them¹⁵ – an obviously insecure method. Others use obvious passwords, such as their spouse’s name, or the same password or PIN for everything.¹⁶ The British survey concludes that the combination of consumers’ failing memories and the increasing sophistication of identity thieves will steadily erode the reliability of passwords as a way of authenticating an individual’s identity.¹⁷

Imposing a mandatory password requirement not only would impose burdens on consumers that far outweigh the benefits, it also would place carriers at a competitive disadvantage vis-à-vis their intermodal competitors not subject to such requirements – both from a cost perspective as well as from a customer care perspective, particularly with respect to customers who object to passwords.

¹⁴ Benjamin Ensor, “How Consumers Remember Passwords,” Forrester Research Inc. (June 2, 2004).

¹⁵ *Id.* at 3.

¹⁶ *Id.* at 3-4.

¹⁷ *Id.* at 6.

While mandatory passwords are a bad idea for any customer segment, they are particularly ill-advised for larger business customers. AT&T typically assigns specific customer care representatives to serve its larger business customers and thus generally can verify customer identity without a password. To impose password requirements on that customer segment would thus offer no conceivable benefit.

To the extent the Commission requires carriers to use passwords as a customer authentication method, the Commission, at most, should require carriers to make passwords available as an option. Even then, carriers should be permitted to use other authentication methods if a customer forgets her password. And, to the extent the Commission *requires* carriers to make passwords available as an option (which it should not), it must ensure that carriers are permitted to recover the costs of implementing any such requirement.

Finally, the Commission should not require carriers to notify customers whenever their password is changed. Under AT&T's existing procedures, to change a password, AT&T's customers have to: (1) provide the existing password; (2) satisfy other authentication criteria if the customer forgets the password; or (3) wait until they receive the password at their billing or e-mail address on file. In each of these scenarios, the password change can only be effected by the party that satisfies authentication requirements, and/or already received notice that the party's password has been changed. Consequently, there is no need to require carriers to provide a separate notice to customers that their passwords have been changed.

2. Customer Notification

Where data brokers and others obtain unauthorized access to CPNI the consequences to individual consumers could be significant. Consequently, even if pretexting and hacking are relatively isolated problems, consumers have a right to know if their private account information

or telephone records have been released without authorization. Given the significant privacy issues and interests at stake, the Commission reasonably could conclude that carriers should notify customers of the release of their CPNI if the carrier determines that a pretexter or other fraudulent third party has obtained unauthorized access to a customer's CPNI. In such instance, the benefits to consumers in receiving a notice¹⁸ would outweigh the costs to carriers of implementing the notification requirement. Carriers, however, should have the flexibility to determine the content of such notices.

These same considerations however would not warrant requiring a carrier to provide routine notification to a customer whenever the carrier receives a request for access to that customer's CPNI or whenever the carrier releases such information. In particular, given that it is not even clear that pretexting or hacking of customers' CPNI is rampant, the limited benefits of such routine notification – whether prior to or after CPNI is released – would be outweighed by the costs (to customers and carriers) of implementing such notification procedures.

A pre-release notification requirement, for example, would negatively impact consumers by forcing them to wait for their carrier to call them back, send them an e-mail or a letter, or provide some other form of notification before accessing *their* information. Such a requirement thus would delay, in some cases significantly, a customer's ability to obtain information and transact business concerning their accounts, as well as preventing them from obtaining prompt resolution of any customer service issues. Moreover, it would prevent customers from obtaining any information or resolving any issues pertaining to their accounts unless they can be reached at the phone number or address (both billing address and/or email address) on file. Plainly, given the realities of today's economy – in which workers are increasingly mobile and two-worker

¹⁸ A customer that receives notice that her account information has been disclosed to an unauthorized third party can take action to prevent further disclosure of her information and to prevent further damage from the release of such information (such as by taking steps to prevent identity theft, etc.).

families are the norm rather than the exception – a pre-release notification requirement would be enormously burdensome and complicated for consumers. Such a requirement also would impose significant costs on carriers by requiring them to expend additional time and resources to resolve any customer service requests and issues.

A post-release notification requirement likewise would impose significant costs and burdens with little, if any, offsetting benefits. Unless the Commission were to require carriers to provide significant detail concerning the circumstances of every instance in which a customer's CPNI records have been accessed, a post-release notification requirement would be virtually useless to consumers, and likely would spawn countless inquiries by customers to determine when their information was accessed and by whom – even where the notification concerned information disclosed to the customers themselves. To the extent the Commission requires carriers to provide detailed notice concerning each and every time a customer's CPNI records are accessed, such a requirement would impose enormous costs on carriers. To comply with such a requirement, AT&T, for example, would have to create a separate organization dedicated exclusively to notifying customers when their CPNI is accessed. AT&T also would be required to modify its systems to develop, deliver and track the notification, irrespective of how such notice is provided. If AT&T were required to provide such notice in a customer's bill – which is the most common method of delivering important customer notifications – AT&T would have to permanently modify its customer bills to reserve an information slot for the notice on the off-chance that AT&T had to provide such notice, even though in two out of every three months (on average) no notification would be necessary. Given the severe spacing limitations on customers' existing bills, as well as the already large number of mandatory notices and other information on those bills, a post-release CPNI notification requirement likely would impose significant

additional costs that would ultimately be passed on to consumers. And since it is not apparent that pretexting and hacking of customer account information is widespread, a post-release CPNI notification requirement could have little utility.

B. Other Measures

Audit Trails. As discussed above, AT&T has in place a variety of policies and safeguards to ensure that employees do not obtain unauthorized access to CPNI. While employee misuse of CPNI does not appear to be a significant issue for AT&T, the Commission nevertheless could reasonably conclude that a requirement that carriers maintain audit trails might be of some value in investigating unauthorized employee access to CPNI. AT&T already maintains such trails as part of its internal security procedures. In particular, in most cases, AT&T maintains a record (audit trail) of each instance in which an employee accesses a system which contains customer information, and has found these records quite useful in investigations involving employee compliance with AT&T's CPNI security procedures. AT&T cautions, however, that audit trails might be of limited utility in the context of pretexting because those trails would only indicate that an employee had accessed a customer's account information at the request of a party claiming to be the customer or its authorized agent. Consequently, audit trails would not necessarily enable investigators to determine the identity or location of the pretexter.

CPNI Certifications. AT&T generally does not object to the Commission's proposal to amend its rules to require carriers to file their annual CPNI certifications with the Commission.¹⁹ While it is not apparent to AT&T that pretexting is widespread, the Commission could reasonably conclude that such a requirement would enable the agency to more effectively monitor the adequacy of carriers' CPNI security measures, particularly if the Commission requires carriers to implement minimum authentication measures. But, if the Commission

¹⁹ NPRM at 29.

requires carriers to file their CPNI certifications, it should give carriers at least until February 1st of each year to both certify and file their certifications for the previous calendar year. The additional 30 days would provide carriers time to verify that their procedures were in fact adequate to ensure compliance with the CPNI rules in the preceding calendar year; a January 1st deadline would not.

On the other hand, AT&T does not believe that requiring carriers to attach an explanation of actions taken against data brokers and a summary of all consumer complaints involving the unauthorized release of CPNI is necessary or appropriate. The existing rules already require a carrier to include in its annual CPNI certification a statement explaining how its CPNI procedures did or did not comply with the Commission's rules. Consequently, to the extent carriers are required to file their certifications with the Commission, the Commission would receive notice of any deficiencies in a carrier's CPNI procedures. Moreover, requiring carriers to provide summaries of actions taken against data brokers and customer complaints could provide fraudsters or pretexters a roadmap to circumvent the carrier's security and investigative procedures, and thus might compromise the security of customers' CPNI. The Commission therefore should not require carriers to attach an explanation of actions taken against data brokers or summaries of consumer complaints regarding CPNI to their annual certifications.

Encryption. The Commission likewise should not require carriers to encrypt CPNI data stored by a carrier, as EPIC proposes. As an initial matter, requiring carriers to encrypt CPNI data would have absolutely no impact on pretexting, which is the focus of this proceeding. Private investigators, data brokers and others who obtain unauthorized access to CPNI through pretexting most often do so by pretending to be the customer whose data they seek to access. Consequently, if a pretexter satisfies a carrier's customer authentication requirements, the carrier

will provide the pretexter CPNI because the carrier reasonably will believe the pretexter is the customer at issue. Plainly, requiring carriers to store their data in an encrypted format will do nothing to prevent this type of fraudulent activity. And while requiring carriers to encrypt CPNI data might be effective to prevent hackers from accessing that data, AT&T has found no evidence that its systems have been hacked. Consequently, requiring carriers to store CPNI data in an encrypted format would impose implementation costs with no corresponding benefits.

Record Deletion. Similarly, limiting data retention by imposing a mandatory record deletion or de-identification requirement, as EPIC proposes, is unnecessary to prevent pretexting because dated CPNI information,²⁰ which is the only data that would be subject to such a requirement, is of little value to entities, such as data brokers and private investigators, that might engage in pretexting. Such a requirement would, however, impinge on the legitimate business needs of carriers, which retain records to respond to requests by law enforcement officials, to develop and design new product offerings for customers, as well as to defend against and resolve potential billing or other disputes. AT&T notes in this regard that it responds to thousands of subpoenas every year from law enforcement officials, many of which extend well beyond the Commission's mandatory 18-month retention period for call-detail records. A record deletion requirement thus not only would prevent carriers from engaging in legitimate business activities, but also could undermine law enforcement, national security and public safety.

A de-identification requirement would raise precisely the same concerns because, without customer-identifying information, customer records are virtually useless to law enforcement.²¹

²⁰ Carriers currently are required to retain toll records for a minimum of 18 months. Beyond that time, such records would likely be considered outdated by a data broker or private investigator.

²¹ Such a requirement could also adversely impact AT&T's ability to serve its customers. Many AT&T customers appreciate targeted marketing. Removal of identifying information could prevent AT&T from effectively and efficiently developing product and service offerings for such customers.

And, worse yet, such a requirement would force carriers to expend significant time and resources to remove customer identifying information from their records.

Modification of Opt-out rules. AT&T strongly opposes modification of the opt-out rules to require carriers to obtain opt-in consent prior to sharing CPNI with joint venture partners or independent contractors. The type of CPNI consent obtained, opt-in or opt-out, is completely irrelevant to the security concerns alleged here. AT&T is aware of no evidence to suggest that joint venture partners and independent contractors are more likely to disclose CPNI to third parties without authorization or that carriers cannot properly control such entities through contracts and otherwise. Moreover, requiring opt-in consent for release of CPNI to joint venture partners and independent contractors would effectively eliminate the considerable public benefits of opt-out procedures, which this Commission has recognized.

The Commission previously permitted carriers to share CPNI with joint venture partners and independent contractors based on opt-out CPNI consent, subject to certain safeguards.²² Specifically, the Commission required carriers to enter a confidentiality agreement with such entities that would restrict their use and dissemination of CPNI.²³ The Commission concluded that these safeguards would ensure that “consumers are protected by the same or equivalent safeguards as those that exist when carriers use CPNI themselves.”²⁴ Further, the Commission concluded that opt-out approval in this context would “directly and materially advance[] the government’s interest in ensuring that customers have an opportunity to approve such uses of

²² *Implementation of the Telecommunications Act of 1996 et al.*, Third Report and Order, CC Docket No. 96-115, RM-11277 (rel. Feb. 14, 2006).

²³ *Id.* ¶47.

²⁴ *Id.* ¶46.

CPNI, while also burdening no more speech than necessary.”²⁵ Underlying this decision was the Commission’s recognition that carriers often use independent contractors to market their services and that an opt-in requirement could seriously disrupt carriers existing business practices.²⁶

All of these justifications remain valid today. AT&T relies to a significant degree on independent contractors to provide marketing, Information Technology (“IT”) ²⁷ and other customer care services such as order handling, post-order customer care, maintenance and repair services. AT&T also provides key communications services, including broadband Internet access services and wireless services, pursuant to joint venture arrangements. Needless to say, such arrangements and relationships are critical to the success of AT&T’s businesses.

AT&T requires all of its joint venture partners/contractors to adhere to the Commission’s CPNI requirements. In particular AT&T requires that they protect the confidentiality of CPNI, use the provided CPNI only for the intended purpose, and not disclose CPNI to third parties unless required to do so by law. These joint venture partners/contractors are expressly prohibited from using CPNI for their own marketing purposes. Violation of any of these requirements constitutes grounds for immediate termination of the arrangement as well as enforcement action by AT&T. AT&T is aware of no evidence that would suggest that these entities do not take these obligations seriously. There is thus no basis for establishing different consent procedures

²⁵ *Id.* ¶32.

²⁶ *Id.* ¶45.

²⁷ Currently, AT&T uses a number of independent contractors to develop and update AT&T software applications and perform other programming functions. These activities often require that these contractors access databases containing customer account information. As the Commission has previously recognized, an opt-in regime could negatively impact the way a carrier does business, which is particularly true in this context. It would be infeasible for AT&T to remove customer account information from its databases to allow IT contractors to make programming or other system modifications, which would be required under an opt-in regime. AT&T’s use of IT contractors has significantly minimized certain of its operational costs. An opt-in regime would force AT&T to perform a large part of its IT-related work in-house, which would be very costly to both AT&T and its customers.

for information shared with independent contractors and joint venture partners than for information used only by a carrier's own employees.

At the same time, disparate requirements could prove costly to implement and might result in customer confusion. Carriers would presumably have to send new notices to customers and possibly modify their existing systems to track additional CPNI consent options.²⁸ Such notices would also likely precipitate numerous customer inquiries as customers are not likely to understand why they have to give express CPNI approval in one instance (marketing by AT&T contractors), but not the other (marketing by AT&T employees and agents), when the bottom line is all the marketing efforts involve AT&T services. A bifurcated consent process might also give customers the false impression that independent contractors and joint venture partners are somehow not trustworthy and thereby induce customers to withhold CPNI consent from which they might otherwise derive significant benefits, including cost savings.

III. APPLICABILITY TO VOIP PROVIDERS

The Commission asks whether it should apply any requirements adopted in this proceeding to VoIP service providers or other IP-enabled service providers.²⁹

The Internet has thrived to date under the Commission's well-established and longstanding policy of regulatory restraint. That policy unquestionably has fostered the explosive development of VoIP and other IP-enabled services. In order to avoid stunting the continued growth of these services, the Commission should remain faithful to its policy of

²⁸ For example, carriers may have to track whether a customer has given opt-in consent to share CPNI only with affiliates or opt-in consent to share CPNI with affiliates, joint venture partners and independent contractors.

²⁹ NPRM ¶28.

regulatory restraint and extend CPNI rules to IP-enabled services only if there is a demonstrated and compelling need.

AT&T does not believe that there is any such need. As AT&T showed in its comments in the pending Title I rulemaking proceeding,³⁰ CPNI requirements have never been deemed necessary for Internet services or application providers, and it is not clear that there is reason for heightened concern with respect to IP-enabled services providers like VoIP providers. While the Commission has retained CPNI rules for telecommunications services it deemed competitive, such as wireless and long distance, here the Commission would be reaching out to impose these protections on an industry that already has functioned well without them. Furthermore, the Commission has recognized, even when deciding to retain CPNI protections, that forbearing from CPNI restrictions can result in benefits to consumers and carriers, such as “promot[ing] a free flow of information from the carrier to the consumer [and] potentially decreasing the carriers’ costs of marketing.”³¹ These considerations are especially important in the market for IP-enabled services where Congress and the Commission have emphasized the need for a nonregulatory approach to encourage broader deployment of these developing technologies.³²

In any event, generally applicable consumer protection laws already apply to providers of IP-enabled services and protect consumers of such services from unfair or deceptive practices. Such laws are designed to prevent deceptive and unfair business, advertising, and billing

³⁰ Comments of SBC Communications Inc., *IP-Enabled Services*, WC Docket No. 04-36 (filed May 28, 2004).

³¹ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14441-42 ¶63.

³² See, e.g., *Amendment of Section 64.702 of the Commission’s Rules and Regulations*, Final Decision, 77 F.C.C.2d 384, 387, 431-32 (1980).

practices by any business, and to ensure that businesses comply with their privacy commitments. Thus, even if the market does not independently constrain such conduct, the existing, generally applicable consumer protection regime provides sufficient security and recourse. Moreover, consumers can easily “vote with their feet” if a provider fails to meet their expectations regarding the security of their records, and choose a provider that has better authentication measures.

Moreover, in response to consumer demand, Internet services and application providers, including AT&T, have voluntarily joined industry-wide groups such as the TRUSTe Privacy Partnership to develop standards for protection of consumer privacy and methods to ensure compliance with them.³³ AT&T and other like-minded providers, in order to attract customers by promising reliable privacy protections, have their privacy practices reviewed for compliance by TRUSTe. And the Federal Trade Commission ensures that companies stand by their privacy policies and promises.

To the extent the Commission concludes that action is warranted to prevent pretexting or other fraudulent activity related to personal telephone records for IP-enabled services, the Commission should only extend those CPNI rules that specifically address such fraudulent activity to IP-enabled services.

³³ For a more detailed discussion, see AT&T Comments, *Consumer Protection in the Broadband Era*, WC Docket No. 05-271, pp. 10-14 (filed Jan. 17, 2005).

CONCLUSION

For the foregoing reasons, AT&T urges the Commission to first validate claims that pretexting and hacking are rampant. Then, if necessary, the Commission should take the actions as outlined above to mitigate the purported harms.

Respectfully Submitted,

/s/ Davida Grant

Davida 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

April 28, 2006