COMMENT OF PRINCETON UNIVERSITY STUDENTS

1. Introduction

We, the students of Professor Edward W. Felten’s Princeton University graduate class Information Technology and Public Policy, respectfully submit the following comments concerning enhanced security and authentication standards for access to Customer Proprietary Network Information (CPNI). We are responding to the request for comments outlined in the Commission’s Notice of Proposed Rulemaking (FCC 06-10).

[Describe our background and training. Spent class time discussing the issues and jointly drafting these comments.]

Recently several news outlets and the Electronic Privacy Information Center (EPIC) have drawn public attention to the sale of CPNI. The advertisements of several data brokers suggest that personal phone records are readily available for purchase online. In response, Congress is considering a number of bills to address the issue (for example, see H.R.4657, H.R.4662, H.R.4709, H.R.4714, H.R.4943, S.2177, S.2178). In this context, we believe the Commission’s consideration of measures to protect the privacy of CPNI is both timely and useful.

Our comments are structured around four methods through which CPNI may be obtained illicitly: pretexting, rogue insider, cyberattack, and theft of records. We consider each breach scenario in turn and then discuss specific policy options to protect telecommunications customers.
Breach Scenarios

Our reading of FCC 06-10 and discussion of possible breach scenarios leads us to the conclusion that there are four methods that may be used to gain unauthorized access to CPNI. Note that our analysis of these scenarios is speculative, and that we are not certain of the ease, efficacy, or frequency with which these methods are used.

1. Pretexting
   In their submission on CPNI to the Commission, EPIC described pretexting as “the practice of pretending to have access to protected records.” Put another way, pretexting occurs when individuals purporting to be a given customer contact telecom providers and formally request CPNI.

2. Rogue Insider
   Another method of gaining unauthorized access to CPNI is acquiring it from dishonest employees of telecom providers. In this instance, we assume that companies selling access to CPNI are offering remuneration to such employees in exchange for privileged information.

3. Cyberattack
   Telecom service providers are also vulnerable to assaults on their computer system and the theft of online information. It may be possible to access CPNI through a cyberattack.

4. Theft of records
   CPNI also may be accessed through the physical theft of records or the hardware storing electronic records. While regular and ready access to CPNI is unlikely through this method, it is still an area of concern.

EPIC notes that many data brokers claim to be able to obtain up-to-date CPNI data in several hours or days. We doubt that cyberattack or theft or records would allow data brokers to do this, so we conclude that data brokers are most likely exploiting either pretexting or a rogue insider to gain access to CPNI.

It follows that defenses against pretexting and rogue insiders are most relevant to the Commission’s goals in this rulemaking. Other modes of improper access, such as cyberattack or theft of records, are worthy of attention in general but are not as relevant to this rulemaking.

In light of these possible attack modes, we now consider the specific remedies suggested by the Commission in the NPRM.

2. Auditing
   [from Jeff Dwoskin’s April 4 post]
The creation of audit trails is an essential element of any comprehensive plan to protect CPNI. Auditing offers a low cost method of preventing the most likely breach scenarios: pretexting and insider theft, as well as some cyber-attacks.

Proposal

We propose that all “large” telecommunications companies — say, those with more than $10 million in revenues — be required to: [This seems overly prescriptive, given our relative lack of knowledge about carriers’ technology setups.]

1. Record all human communication that results in access to CPNI, such as a customer seeking his calling records
2. Record all electronic access of CPNI, such as internal accesses, outside marketers or third party partners
3. Record the purpose of each access, distinguishing between internal uses of CPNI and disclosures to consumers, partners or third parties
4. Make these records available to customers upon request
5. Inform customers when anomalous access is detected
6. Use these audits to monitor and improve employee and third party handling of private information
7. Retroactively analyze and investigate suspected breaches to detect attack patterns and eliminate vulnerabilities
8. Maintain the integrity of CPNI audit logs, and preserve audit logs for 5 years or as long as the CPNI data is kept, whichever is longer.

Cost

The proposal balances the requirement of universal security with sensitivity to the limited resources of small firms. For large telecommunications firms, making records of access to sensitive data should be minimally costly, since these companies already make audits for certain types of access. The cost of analyzing and improving security systems should vanish in time [should say why they will vanish] and, in any event, will pale in comparison to the value it provides. Small companies may find it more difficult to create auditing systems, but will compensate by having a tighter rein over their employees. Moreover, once large companies adopt stringent security standards, CPNI theft will become financially unviable, so it is not necessary for every company to zealously guard its data so long as most of the market does.

Integration with other security measures

Audits, while moderately useful in their own right as a deterrent and a tool for law enforcement, are most effective when paired with other security measures. The most obvious connection is to customer notice, which we discuss below in Section 3.

Beyond consumer notification, automated anomaly detection should [“should”, or “may”?] be used to flag suspicious access and discover patterns of theft. This will deter
insiders from accessing abnormally high numbers of accounts and will force outside thieves to vary their method of access, which should be quite costly. A record of what techniques pretexters use could also be used to train customer service agents and improve anomaly detection.

The final realm for integration would be with preemptive filtering. If audits reveal that thieves tend to use payphones or cell phones, companies could insist that access be done from a land line that can be more easily traced. If certain cities harbor CPNI thieves, more stringent security measures could be implemented in that city. If certain thefts occur at certain times, companies could staff their call centers with more experienced employees during peak theft hours. While some of these measures could be effective, their expense and the risk of consumer inconvenience make them inappropriate for Commission mandates, but rather should be left to be adopted voluntarily by companies.

[Notes on the auditing section: The proposal section is complete. we have to do a little more editing on the last 2 sections.

To add to text:
- integrity - protect from modification by people making accesses.
- purpose - internal marketing, customer service request, outsourced services, third party partners, etc

Note: statute of limitations on mail and wire fraud is 5 years. (10 years for financial). 2 years is a reasonable compromise for other communications.
We don’t know what’s appropriate for preserving/retaining human communications. might be at discretion of the company as they find useful for investigations. ]

3. Notification

Public reaction to the release of CPNI has shown that the public should be dissatisfied with the wireless carriers protection of consumer information. The failure of the companies to protect that information suggests that – at a minimum – if the information cannot be protected, consumers should at least have a right to know when their CPNI has been fraudulently transferred, even when that notification is ex post facto. Our study of notification policies has focused on the idea that notification of security breaches involving CPNI is useful to prevent pretexting – or future pretexting, but notification to consumers is unlikely to prevent the rogue insider, cyber attack or physical theft security breaches. A consumer who understands his commonly used password has been stolen is empowered to protect himself against future uses of his identity. For this reason, we support EPIC’s proposal that notification be used as a tool to protect CPNI.

CTIA and the wireless carriers generally failed to provide comment on the costs or possible benefits of providing consumers notification of any level, other than to note that they believe additional Commission rules to be unnecessary. CTIA urged stricter
enforcement of existing laws and, naturally we concur. But stricter law enforcement is not enough.

Several key questions must be addressed: in which cases should consumers be notified and by what means. Our review suggests that consumers should be notified in the event of a security breach – in other words, not when CPNI is transferred for legitimate business development purposes but when the transfer has been deemed wrongful, as in the types of breaches described above. We believe that requiring carriers to notify customers of routine CPNI transfers is too burdensome and adds little value to the consumer who wants to protect his CPNI. For the purposes of commenting to the Commission, we believe that CPNI can be divided into two areas: call service records and personal records. Only the transfer of personal information or personal information tagged with the call records constitutes the necessity of notifying the consumer.

Carriers have several readily available means for notifying consumers of a breach. First, consumers can opt-in/opt-out of receiving such information. Second, notification could be as simple as a line item on a billing statement (electronic or hard copy) or via direct communication – voicemail, email, or letter.

There is a strong case to be made for regular notice, on the grounds that it creates incentives for carriers to act more securely and with greater vigilance. Further, there is a normative claim that end users have a right to know when their data has been wrongly transferred, irrespective of whether or not they can get it back. Finally, for certain types of sensitive data that should not be regularly transferred (for example detailed call logs), we recommend notice for preauthorization can reduce leaks and should not be overly burdensome.

4. Encryption

Encryption is the process of obfuscating information so that it is unreadable without additional knowledge. Generally the special knowledge required to discover (decrypt) the original information is knowledge of which process was used to encrypt it, as well as knowledge of a specific piece of information, a ‘key,’ to unlock the encryption. When encryption is done well it is generally not possible to uncover both these pieces of information simply by examining the encrypted data.

Where Encryption is Effective

It is clear that a carrier would need to have at its disposal a means of decrypting the data. We recognize that CPNI data is used for legitimate business purposes, and so it is meaningless if it cannot be made readable. Some employees at the carrier must have access to a decryption device in order to perform their jobs.

Carriers also provide means of giving users access to their own CPNI. We do not dispute that these means should be available; we only note that CPNI cannot be disclosed to the
user in encrypted form or they would not be able to read it. In order to provide such a
service, carrier’s customer service representatives must have at their disposal a method of
releasing decrypted CPNI data to the user to whom it belongs.

It follows that encryption is emphatically not a solution to the problems of pretexting and
dishonest insiders. If someone has convinced a customer service representative that they
should be given certain CPNI data, the data will be given to them in plain text. If a carrier
employee is inclined to feed CPNI data to data brokers they will be able to do so if they
have been given access to decrypted CPNI data in order to perform their job.

We believe that encryption of stored data is an effective counter-measure against two
methods of acquiring CPNI data: cyberattack and physical theft of data.

**Encryption and Cyberattack**

In examining the effectiveness of encryption in countering cyberattack on carriers it is
necessary to divide cyberattacks into two categories: attacks carried out by interacting
with a carrier’s web site and attacks in which an attacker gains direct access to a carrier’s
database.

EPIC notes that an attacker might crack a user’s online account with the carrier in order
to obtain CPNI data. A carrier’s web site, like a customer service representative, must be
able to give a user’s decrypted CPNI data to the legitimate customer. An attack on the
web site might allow an attacker to bypass the authentication mechanisms of the web site
in some way. Such attacks are analogous to deceiving a customer service representative
by pretexting. Encryption is not effective against this sort of attack, as the web site, like
the customer service agent, will simply display the decrypted CPNI data once convinced
(falsely) of the user’s identity.

We do agree that encryption could help in mitigating the damage dealt by a cyberattack
where an attacker fraudulently gains direct access to a carrier’s database. In such an
attack the attacker would be forced to go to the additional trouble of figuring out which
encryption scheme and which key were used.

While encrypting data can help against some forms of cyberattack, we are not in a
position to comment on the prevalence of such forms of cyberattack as means of
acquiring CPNI data relative to other methods like pretexting.

**Encryption and Physical Theft**

It is common practice for databases to be copied and stored for recovery in case of an
accident or some need for older data. There is no doubt that, if backup copies were
encrypted, physical theft of backups would be a pointless endeavor. We doubt, however,
that physical theft is the primary method, or even a common method, of illegitimately
acquiring CPNI data.
As noted above in the Introduction, we doubt that physical theft of records could allow data brokers the kind of on-demand access to CPNI that they apparently have. Mandating encryption to guard against physical theft might be a good idea, but if the Commission’s immediate goal is to counter on-demand sale of CPNI by data brokers then an encryption mandate would be mostly unrelated to the goal.

**Carrier’s Reservations and Responses**
Carriers have commented that data is already encrypted ‘where appropriate’ and that encrypting stored records would be costly. We find these two statements contradictory. If some data is currently encrypted, then infrastructure for the encryption and decryption of data must already be in place. We do not think it likely that it would be extremely costly use in place infrastructure to encrypt and decrypt additional data.

Carriers have also argued that encryption would slow legitimate inquiries for CPNI. We do not believe this to be true. There are varying types of encryption, but it is possible to choose a method that is both secure and fast. For example, the Advanced Encryption Standard (AES) mandated by NIST offers ample security and speed for this purpose. In the case of a customer interacting with a carrier’s web site we believe that the communication time between the web site and the customer’s computer will be far greater than the time required to decrypt the relevant CPNI data. As such, customers should not experience any noticeable slowdown, nor should carriers’ computer systems be burdened by the need to decrypt.

We believe that the most powerful criticism of encryption as a means of mitigating inappropriate disclosure of CPNI data is that encryption provides benefits largely unrelated to that goal. As discussed above, encryption cannot stop pretexting or dishonest insiders, and is only effective against some forms of cyberattack. This does not mean that such forms of cyberattack are not worth guarding against.

**Recommendations**
We find it somewhat troubling that CPNI data is encrypted ‘where appropriate,’ not because all CPNI data should be encrypted, but because this represents individual carriers’ understandings of which pieces of CPNI data are worth protecting. If only to encourage baseline security practices, we believe that categories of CPNI data that must be encrypted should be established.

We recommend that any piece of CPNI data that might be used as personal identification of a customer (i.e. name, address, phone number, social security number) should be encrypted. In this way CPNI data that is acquired via cyberattack would not be valuable to data brokers as they would be unable to tie records to people without decrypting the data.

**(Slightly) Technical Analysis**

[Not sure how to incorporate this subsection. It’s relevant but it doesn’t fit together neatly with the previous text.]
As noted above, it is “computationally infeasible” for an outsider to be able to determine both the “encryption key” as well as the process in which the key was used to encrypt the information into ciphertext. However, that is not to say that the use of encryption in a communications system is guaranteed to make the system secure. For example, SSL, which is a prominent security protocol used in nearly all secure online connections (https://), involves a public key exchange. A notable method of key exchange, Diffie-Hellman, is vulnerable to a “man-in-the-middle” attack in which someone receives and then re-sends all traffic involved in the exchange without ever being detected. Thus, a system of communication is vulnerable, even in spite of the use of clever encryption methods.

Also, there are some concerns on behalf of the carriers that encrypting too much information will cause the regular access of common information to take too long. As we will see, this is not a legitimate concern as the bottleneck on the amount of time it takes to access your own personal information is not the encryption protocol in use, but the actual speed of the connection.

We propose the 3-part model shown at the end of this passage.

This model assumes that the carrier is large and has a certain level of technological capabilities, namely the database and web server are separate machines. This model also assumes that the end user is authenticated, that is to say that the person behind the client machine is who he/she claims to be, and their password’s integrity is maintained.

The first point of concern is the channel between the client and the web server. A security protocol named SSL is a nice way for a client to establish a secure connection through the use of a message authentication code, or a MAC, which can verify the integrity and authenticity of messages traveling back and forth, and a “handshake” between the two devices that confirms that each node is a trusted party. SSL, when used in conjunction with http, forms a secure connection that is believed to be secure enough.

The next point that is a potential security concern is not the web server, but the database itself. Fortunately, the web server is not an effective spot for an attack to steal sensitive information, it is only effective for creating a Denial of Service situation. If an attack were waged on the database, then an intruder to the system could easily steal tons of extremely valuable information in a short time. Thus, it is absolutely imperative that the raw data sitting on the database server resides in an encrypted form. Encryption today is so strong that the Earth would likely end before the cipher could be cracked.

The final concern about encrypting information is that of look-up speed and accessibility. It turns out that the bandwidth capabilities of the client’s connection to the web server trump the time it takes for the data to be looked up/encrypted. This fact makes it entirely possible for carriers to efficiently/effectively implement encryption for security purposes.
5. Consumer-Set Passwords

In response to the Commission’s inquiries regarding passwords, we believe passwords can be an effective deterrent against unauthorized access to user’s phone records. Of the different ways to acquire another person’s phone records, passwords would only be effective against pretexting. However the CTIA itself has stated that “overwhelmingly, the vast majority of cell phone records are being fraudulently obtained through the use of ‘pretexting.’” Pretexting is when one attempts to obtain information by lying about one’s identity or authority to access this information. Because the CTIA itself acknowledges that pretexting is a rampant problem steps should be taken to attempt to curb pretexting. One such method is requiring a special password from users in order to access their records.

While passwords can never be 100% effective they do provide an important first line of defense against those who wish to illegally obtain other people’s phone records. In discussing the effectiveness of passwords there is a necessary tradeoff that must be acknowledged. The stronger a password is the more of a burden it will place on a legitimate user. For example one could set up a system that required three separate passwords unique to this system made up of numbers, letters, and symbols. While this would provide a high level of security it would also require the user to remember each of these passwords. On the other hand, one could choose a password that would be easy to remember which they use often such as their mother’s maiden name.

We also feel it is important to acknowledge that different customers would prefer a different balance between security and convenience. Some might be unconcerned with who has access to their record of calls as long as they have easy access. Others might prefer the hassle of a complicated set of passwords in order to help ensure their information is not compromised. We believe that any solution involving passwords must attempt to address both of these potential customers.

Finally, any potential solution must not only address the passwords themselves but also the system for dealing with lost passwords. The password recovery mechanism can often act as a back door for those wishing to gain access to otherwise secure information. As with passwords themselves, we believe there should be some flexibility for the user. If the user prefers tighter security then the procedure for dealing with lost passwords should be more complex and more secure than if they prefer convenience.

With these considerations in mind we propose the following solution. Existing and new users would initially be given a medium level of security. This would mean they would have a user-defined password that would be unrelated to any personal information. Also, if they forgot their password they would have to physically send a written request to the phone company requesting their password be reset. If the customer preferred there would also be a heightened level of security for which there would be two passwords. One password assigned by the phone company and one chosen by the consumer. Again a physical letter would have to be sent to the company in order to reset the passwords. When the passwords are reset a letter would be sent to the billing address informing the
customer of the new passwords. The customer could even request that their phone records only be made available by a written request. Their record would then be sent to their billing address. This would provide the highest level of security against pretexting. Finally, we would have a low level of security option for which the user could choose a simple password and the system for resetting a lost password would be tied to some piece of personal data. In order to get this level of security the customer should be required to sign a waver indicating they understand the risks involved with such as system. In this way, we aim to allow the customer to choose what level of security is appropriate.

The major weakness with this system is in the users themselves. Many will not be concerned with the heightened risk until their information is actually targeted. At this point they likely will prefer a heightened level of security. Some will not fully understand the risks with the lower level of security until it is too late. However passwords would likely prove ineffective for these users anyways because they will likely store them in such a way that will be easy for would be data minders to find.

The CTIA is adamantly opposed to any new rules being imposed on them to protect data. Rather they assert that the most effective measures against pretexting would be to strengthen the laws against pretexting. In essence, they prefer an offensive approach which targets the pretexters rather than a defensive approach which would target themselves. While they are obviously motivated by their own self-interest their arguments should be addressed. It is important to stress that requiring more effective passwords and targeting pretexters are not mutually exclusive. Rather the two measures would act as complements. While it is illegal to steal a car it would be foolish for the owner of the car to leave the car unlocked and the keys in the ignition. As discussed above passwords will not and cannot be 100% effective. However, they are more effective than no passwords at all. While one could argue they provide a false sense of security the solution is not to eliminate the security altogether but to attempt to inform people that it they are not 100% effective.

6. Limiting Data Retention

[need to turn this into prose]

**IDEA:** Setting a multi-stage, maximum time for telecommunications’ company’s retention of personally identifiable telephone usage data in the active network (with only archived access remaining) as a strategy for reducing the vulnerability of individuals to attacks on their personal telephone usage data.

Specifically, we think that a tiered system of data removal with the following steps could be an effective strategy.

[Note that appropriate timelines for the completion of each step would be left to industry and regulators to determine. Here we simply offer a general framework.]
**Stage 1:** Remove all records from the active online network to an archive that is encrypted, or which incorporates usage storage of physical records off-site.

**Stage 2:** Delete the text messaging and video messaging trails.

**Stage 3:** Remove select personally identifiable information from any electronic archives-example: remove parts of the call from and call to numbers leaving only the area codes and remove data on the geographical location of the customer at time of call.

**Stage 4:** Complete removal of all personally identifiable information from the provider’s network (ex. Customer name, address, SS#, customer #, etc) in such a way that complies with existing rules and regulations (ex. Patriot Act requirements or requirements for Law Enforcement purposes).

We evaluated this strategy on the following criteria:

a. Usefulness (against each of the breech scenarios)

b. Practicality

c. Cost

d. Drawbacks

e. Other Important Considerations

a. Usefulness (against each of the breech scenarios)

We think that the strategy outlined above may be particularly useful for the following breech scenarios: 1 (pre-texting), 2 (insider), and 3 (cyber attack). Since archived records still remain somewhere (in an encrypted database offline, or in a warehouse for example) physical theft may remain as a problem, although arguably a very rare one. Regarding breech scenario 2, where an insider is compromising access to records, theoretically someone could request access to records on a regular basis just prior to the records’ transfer to archives and thus build and maintain an extensive record of individuals’ telephone activity. This kind of diligent pursuit of records may not be common or may be detectible in the audit process.

b. Practicality

As an issue of practicality, we think that limiting data retention is a practical approach with low costs and which requires a low level of interference on the part of the regulator.

c. Cost
It is our understanding that the economic cost of keeping the data around is fairly low (storage costs). We also believe that the costs associated with getting rid of the record are low. The deletion process can be automated and proceed without much additional direction.

d. Drawbacks

Deletion of the data may have some associated negative externalities for the criminal justice process where access to the personally identifiable information stored in company’s phone records is helpful. However if storage of data is not required by law then the security benefits to be derived may justify these externalities.

e. Other Important Considerations

*We would like more information about the average length of time that records with personally identifiable information are currently being kept as well as why they are being kept this length of time.

*We want to make certain that we have a clear view of what pieces of information are actually being collected and associated with customers’ activities. We currently think that the following information is included (name, SS#, customer #, address, time of call, duration of call, location of cell customer when call was made, number called, number of caller).

*Should there be a difference in the rules regarding limiting retention of records for corporations versus government entities versus individuals? Our group is presently undecided on this issue.

*We think that companies should have to make their data retention policies public so that customers can use them as a basis for choice of an appropriate provider.

7. Impact on Small Carriers

We think that there might be a disproportionate burden on small carriers if in order to meet the new standard of security, these carriers must upgrade their technology, at least to a greater extent than large carriers. Large carriers, on the other hand, are likely to already have the best technology available, as well as experts on hand (e.g., chief technology officers) who know how to operate and install this technology. Therefore, requiring some minimum level of encryption, as we recommend, might force small carriers to spend money on new technology, whereas large carriers might not need to make such expenditures because they already have sufficient technological capabilities.

If placing an undue burden on small carriers is a big concern, then we recommend the following. Instead of enacting legislation which applies equally to all carriers, it might be wise to enact legislation which affects carriers differently depending on their size. Or alternatively, we could pass legislation which affects only large carriers. Given that these
carriers presumably represent a substantial share of the telecommunications market, such a policy would have a significant impact (i.e., protect a large fraction of the consumer population) without imposing additional costs on small carriers.

8. Conclusion

This rulemaking focuses, appropriately, on the relatively narrow issue of improper access to CPNI via data brokers, the broader issue of security for customers’ telecommunication data will persist, and is likely to intensify over time. We commend the Commission for its attention to this matter.