Before the
FEDERAL COMMUNICATIONS Commission
Washington, DC 20554

In the Matter of

Electronic Privacy Information Center

Petition for Rulemaking to Enhance Security
and Authentication Standards for Access to
Customer Proprietary Network Information

CC Docket No. 96-115

RM-11277

To: The Commission

COMMENTS 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).

We are a diverse group of students drawn from departments across the University. This submission is the synthesis of class consideration and discussion of the Commission's Notice of Proposed Rulemaking in particular and CPNI in general.

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 recommend five 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 of 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

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 recommend that the Commission take a number of steps in regards to auditing of access to CPNI. First, telecommunications companies should be required to **record all electronic access to CPNI**, distinguishing between internal uses and disclosures outside of the company (to consumers, outside marketing, third party partnetrs, etc). This record would indicate the purpose of each access (e.g. billing, internal marketing, customer service request, outsourced services, third party partners).

Second, consumers should have the **right to request a complete copy of their records**, and should **receive automatic notification of all disclosures** of their CPNI. Customers would be able to report suspicious disclosures to the company which may trigger an internal investigation. Furthermore, companies should be encouraged to use automated anomaly detection as another means of detecting fraud and notifying consumers. It would be helpful for investigations if the companies were encouraged to also kept recordings of all human communications (e.g. phone calls to customer service) for a reasonable length of time when complaints may arrive. These investigations may reveal suspected breaches and help detect attack patterns. This information can be used to eliminate vulnerabilities and develop better procedures for handling private information.

Third, telecommunications companies should be required to **maintain the integrity of the audit logs and preserve them** for 5 years or as long as the CPNI data is kept, whichever is longer. This would give adequate time for breaches to be detected and investigated.

Implementation and Costs

We expect CPNI to be stored electronically so that an audit record can be automatically generated by a computer anytime the information is accessed. We recommend tying this process with employee computer accounts so that there is no ambiguity as to who is accessing the file. The purpose of an access (e.g. internal marketing, customer service request, outsourced services, third party partners) and type (e.g. use or disclosure) may be automatic based on the system or employee's role (e.g. billing dept) or may be entered manually (e.g. by customer service reps). This should be logged in addition to basic information such as time or the employee accessing the data. The recording of purpose adds an extra check in the process and provides accountability. Lastly, the system for logging accesses and storing those records needs to be kept secure and only a limited number of high level IT administrators should be able to make extra-system modifications to those logs.

We suggest that these proposals be applied to large telecommunications companies, as defined by the Commission. This balances the requirement of universal security with sensitivity to the limited resources of small firms. For large companies, making records of access to sensitive data should be minimally costly, since these companies already make audits for certain types of access, and CPNI itself is a type of audit log.. Small companies may find it more difficult to create auditing systems (which may not be a feature of off-the-shelf software), 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. Allowing customers to access records of all accesses to their CPNI and notifying them when any information is disclosed outside of the company, will improve the chance of catching thieves. It will also increase awareness among consumers of how their data is used, potentially prompting them to take additional security measures.

Beyond consumer notification, automated anomaly detection 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 preemptive measures could be effective, their expense and the risk of consumer inconvenience make them inappropriate the Commission to mandate, but rather should be left to be adopted voluntarily by companies.

3. Notification

Public reaction to the widespread availability of CPNI has shown that the public should be dissatisfied with the wireless carriers’ protection of consumer information. The failure of the carriers to adequately 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. Our study of notification policies has focused on the idea that notification of security breaches involving CPNI is useful to prevent pretexting and potentially rogue insiders, but such policies are unlikely to address cyber attack or physical theft security. Nevertheless, given the predominance of pretexting as a suspected means of CPNI access, we support EPIC's proposal that notification be used as a tool to protect CPNI. We consider three cases of CPNI data: large scale breaches, routine transfers, and pre-verification for highly sensitive data.

The first category involves situation where large-scale security breaches have led to exposed personal information for many people. These breaches of CPNI are likely to result from cyber attacks or physical theft. We believe there is a strong case to be made for notifying all affected users in these cases. In addition to fulfilling the public's right to know about such incidents, such notification would also encourage companies to institute better security measures to avoid public embarrassment. Numerous states already have independently proposed legislation for such cases. We respectfully support such legislative efforts, but question whether additional rules from the Commission might be redundant, given these legislative efforts.

Far more pervasive than cases of massive theft are routine transfers of CPNI. CPNI may be frequently transferred for legitimate business purposes. We do not know the extent of such transfers, but it is easy to imagine that within a carrier, CPNI may be transferred between marketing and billing departments. 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. The costs may be very high for the carriers, and the benefit is dubious. At the very least, if carriers are required to notify users of routine transfers, it might be advisable to give consumers the choice about whether or not to receive notification.

Finally, we consider the case of transfers of highly sensitive data that should not be routinely transferred. As an example, consider a personal call log tagged with identifying information. While users may occasionally request such information, occasions of this should be irregular. Since these types of accesses are most susceptible to pretexting, we believe that notification policy could be most effective here. 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. Carriers could freely choose from any number of reporting options; for example, including a byline on a regular account statement. Another possibility is using known secure channels to pre-verify these sorts of data releases. For instance, this could take the form of fulfilling requests only from the phone number associated with the account. Alternatively, carriers could contact the affected customer in a known way (email, phone call or text message, for example) and confirm that the user is requesting the release of the sensitive data. While pre-verification of this sort may be the most effective *preventative* method against pretexting, there is the concern that it could be significantly burdensome to the consumer and to the carriers.

Thus, we find strong evidence that the use of notification can reduce the occurrence of fraudulent release of 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. We have outlined three different types of transfer which we believe are best addressed by varying levels of notification requirement.

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 of stored data is not effective against this sort of attack, as the web site, like the customer service agent, must display the decrypted CPNI data once convinced (falsely) of the user’s identity.

We do agree that encryption of stored data 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.

A (Slightly) Technical Review

As noted above, it is generally not possible for an outsider to determine both the ‘encryption key’ as well as the encryption method. However, that is not to say that the use of encryption is guaranteed to make a 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 may be vulnerable, even in spite of the use of clever encryption methods.

It is also worth noting that, while encryption of stored data will not serve to counter attacks directly on a carrier's web site, there are encryption methods (like SSL) which can we used to secure the channel between the carrier's web site and the customer's computer. SSL and other methods are widely employed in Internet commerce and should certainly be encouraged where they are not already present.

We suggest that there be some incentive for carriers to employ industry standard security practices. Such practices might include the use of SSL for secure Internet data transfers as well as the physical separation of web server(s) from the computer(s) maintaining the database. Without good general security practices the encryption of stored data might gain nothing.

Carriers' 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. Cyberattacks in which an data broker gains access to the carrier's database might be infrequent (we do not know). However, they will be devastating to the privacy of CPNI data if they do occur.

Suggestions

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. We believe that categories of CPNI data that must be encrypted should be established.

We suggest 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.

We also suggest that there be some effort to encourage strong technical security practices among the carriers. We are not experts in the field of computer security and so we are not in a position to describe what such practices should be, so we propose that some effort be made to discover what should be required of carriers in this respect.

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 tired 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

We respectfully suggest that the Commission encourage telecommunications carriers to adopt a public data retention policy that limits storage of CPNI only as long as operationally necessary. An effective data retention policy will limit both the extent and severity of attacks in the event that the system has been breached. This will not, by itself, solve the consumer privacy problem. We also respectfully suggest complementing this policy with a two-tiered data deletion model.

In the first stage, we respectfully suggest that the Commission encourage carriers should strip all personally identifiable information from CPNI records after the legally required 18 month duration. [CITE 47 CFR 42.6] This includes, but is not limited to: all 7-digit phone numbers called and received; subscriber name, social security number, and contact information; and services purchased such as call forwarding or voice mail.

Stripping CPNI in the first stage protects consumers against extensive pretext, insider attacks and cyber attacks for information that carriers no longer need. We understand that carriers are concerned about long-term dispute resolution, but this rare occurrence should not be at the expense of privacy interest of their consumers.

In the second stage, we respectfully suggest that the Commission encourage carriers to purge individual call information by aggregating and then deleting the remaining record data. As a general guideline, the second stage could begin after 36 months. This includes, but is not limited to: all phone number area codes; individual call times and durations; and physical location of calls if the service is wireless.

The second stage safeguards consumers against sophisticated call analysis attacks in which customer identity could eventually be deduced. We understand that carriers may be maintaining this data for statistical purposes. The aggregate information will still allow carriers to collect general trends and statistics about their network, but should make it impossible to trace sensitive call information back to individual consumers.

We also respectfully suggest that the Commission encourage carriers to publicly disclose their data retention policies. This will allow consumers to make more educated decisions about their privacy risks when choosing an appropriate provider. Public disclosure would enable market forces to pressure carriers into adopting privacy-friendly retention policies in an effort to attract new customers. Note that a public retention policy would not assist wrongdoers by contributing to a "roadmap" for future attack.

The cost associated with data deletion is low for carriers since the deletion process can be computer-automated and data deletion is encouraging carriers to spend less by maintaining less storage data.

Moreover, we suspect that even an aggressive policy would not interfere significantly with law enforcement efforts since CPNI must already be retained for 18 months [CITE 47 CFR 42.6]. Carriers have no legal obligation to better assist law enforcement, but they do indeed have a legal responsibility to their own consumers to minimize unauthorized data disclosure.

Commenter CTIA opposes data destruction by claiming that "no security principle makes older records more susceptible or new records less susceptible to fraudulent disclosure." Though this is true, destroying data will guarantee that fraudulent disclosure of older records will never occur in the future — the policy of deletion represents the best security principle possible. We point out that no carrier comments thus far submitted have expressed any strong objections to the data retention guidelines proposed in EPIC's petition. [CITE original EPIC petition]

We are also concerned about the security of other stored communications data such as voicemail, text and photo messages sent among consumers. We have little public information as to whether carriers cache this sensitive data and ask the Commission to consider if this data is subject to the same rules as CPNI during the rulemaking process.

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

We respectfully suggest that the commission take five key steps to protect telecommunications customers:

1. Require large telecommunications carriers to create audit trails
2. Require telecommunication carriers to notify customers in the event of a security breach
3. Require telecommunication carriers to encrypt any piece of CPNI data that might be used to personally identify a customer
4. Require telecommunication carriers to provide consumer-set passwords
5. Require telecommunication carriers to limit data retention

Together these measures would reasonably safeguard customer privacy without unduly burdening telecommunication carriers. Table 1 shows how the remedies address each of the different breach scenarios.

Table 1. The proposed remedies' effect on the four breach scenarios.

	Breach Scenarios			
Remedies	Pretexting	Rogue Insider	Cyber attack	Theft of records
Auditing	✓	✓	✓	
Notification	✓			
Encryption			✓	✓
Consumer-Set Passwords	✓			
Limited Data Retention	✓	✓	✓	

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.