Before the
Federal Communications Commission
Washington, D.C. 20554

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

To: The Commission

REPLY COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

June 2, 2006

The Electronic Privacy Information Center (EPIC) respectfully submits these reply comments concerning enhanced security standards for customer proprietary network information (CPNI).[1]

EPIC first petitioned the FCC to enhance its rules regarding security for CPNI in August of 2005, when it called the Commission's attention to the widespread sale of consumers' phone records online. In March of this year, the Commission granted EPIC's petition and initiated the present rulemaking.

I. Scope of Problem and Harms

EPIC believes that the scope and scale of CPNI sales is more than sufficient to justify rulemakings curbing its use. Though some telecommunications carriers may question whether pretexting is a "rampant" problem,[2] others have readily noted that they receive a high volume of pretexting calls. In comments from earlier in this proceeding, for instance, Verizon Wireless has noted that it receives pretexting calls "several times a

[1] Notice of Proposed Rulemaking, Customer Proprietary Network Information, 71 Fed. Reg. 1317 (Mar. 15, 2006) (NPRM).
[2] Comments of AT&T Inc. at 10, filed Apr. 28, 2006.

day."[3] The scope of the problem is made even more apparent when a complaint by Florida's attorney general reveals that Verizon Wireless received, within a one-month period, over 5,100 calls from a single number associated with an alleged pretexter.[4] Such numbers should leave the Commission no doubt that the disclosure of phone records is a rampant problem.

Moreover, while EPIC recognizes that such illegal disclosures would not occur without the fraud committed by pretexters and their customers, it is poor security practices that enable such a volume market in CPNI to emerge. As such, poor security practices by carriers contribute significantly to the improper sale of customers' personal calling information, and should be addressed by appropriate rules mandating baseline security standards.

Many carriers have commented on the cost of implementing certain security measures, and have claimed that these costs are disproportionate to the harms generated by pretexting. EPIC urges the Commission to recognize that it is consumers, far more than the carriers, who bear the harms of pretexting. These harms extend beyond the financial, such as when data brokers acquire information on victims of stalking or domestic violence.

II. Passwords and Authentication

Some comments note that mandating passwords may create problems, such as when consumers forget passwords, or choose passwords that are easily guessed or used across accounts.[5] However, specified strings of characters are not the only means of generating password-type authentication. As mentioned in EPIC's comments to this proceeding,[6] a system of "shared secrets" prompts can ensure that consumers will have an easily remembered method of authentication that makes use of non-public information. So long as the prompting questions do not cover information that is available in public records (such as favorite colors or childhood pets), such shared secrets do not offer the same risk as biographical methods of authentication (such as birth date, address, or zip code).

EPIC recognizes that there may not be any one best solution to the evolving problems of authentication, but a baseline standard for security should disallow particularly egregious bad practices, such as using a customer's SSN or birth date for authentication.

---

[3] Comments of Verizon Wireless, at 4, filed Oct. 31, 2005.
[4] Complaint, ¶ 19, *State v. Global Information Group, Inc.*, http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6M9RY3/$file/Global_Complaint.pdf.
[5] Comments of AT&T, Inc. at 10-11, filed Apr. 28, 2006; Comments of CTIA at 13, filed May 1, 2006; Comments of the National Association of State Utility Consumer Advocates at 16, filed Apr. 28, 2006.
[6] Comments of EPIC, *et al.* at 13, filed Apr. 14, 2006.

III. Audit Trails

Carriers have commented on audit trails by decrying their cost, as well as their inability to prevent pretexters from obtaining information.

The cost of maintaining mandatory audit trails would not increase at all for some telecommunications carriers, who have acknowledged that they already maintain extensive audit trails.[7] Other carriers note that they keep audit trails that track all instances of customer requests for information.[8] Since a significant portion of pretexting appears to take the form of customer requests, such measures, already in place, would be ideal for tracking and identifying the calling patterns and characteristics of pretexters.

CTIA claims that an audit trail is futile, since it would only reveal that the carrier had disclosed information to the customer.[9] However, this ignores the forensic value of an audit trail. Customer service representatives particularly susceptible to pretexting could be identified and singled out for additional training. ANI information could be correlated with the trail to identify the numbers of likely pretexters and flag them for further investigation. The audit trail could assist in criminal investigation where the number of the telephone customer adversely impacted would be readily available.

In addition, the problem to be addressed by the Commission is the improper and illegal disclosure of consumers' CPNI, regardless of the means by which this happens. The focus on pretexting, while useful, can also obscure the fact that this is not the only threat model to CPNI confidentiality. Audit trails are vital tools for detecting wrongdoing by insiders, whether such actions are deliberate breaches of security or a lack of proper training and procedure. The mere fact that the industry would adopt audit trail procedures would almost certainly discourage some illegal activity.

IV. Notice and "No-Release" Requests

Comments have discussed two types of notice for customers: preventative notification, which requires customer consent before disclosing call records or personally identifiable information; and post-breach notification, where customers are informed after data is improperly disclosed. Comments have also addressed the suggestion that consumers be allowed to request that their records not be released except under specified conditions.

EPIC believes that consumers should always be notified if a carrier is aware that information has been, or was likely to have been, disclosed improperly. If a carrier is fully aware that an improper disclosure has occurred, it would be remiss in its responsibility to the customer if it did not inform him of the breach.[10] Customers who

---

[7] Comments of AT&T at 14.
[8] Comments of Verizon at 13, filed Apr. 28, 2006.
[9] Comments of CTIA, at 14.
[10] *See also* Comments of the Department of Justice at 14, filed Apr. 28, 2006.

have particular reason to fear disclosure of their CPNI are placed in a far more dangerous position if carriers willfully ignore a security breach of the customer's information.

As for preventative notification, CTIA claims that the high volume of customer requests for information (100 million a year) would render notice "ineffectual" and "annoying" to consumers.[11] However, given the vast number of accounts, each consumer likely requests records a very limited number of times, and would be easily warned if he receives a notice for a disclosure he did not request. The likely infrequency with which individual consumers request statements outside of their normal billing process also undermines AT&T's argument that release notification would "spawn countless inquiries by customers" even if the customers themselves had requested the data.[12]

CTIA further claims that a lack of lawsuits, complaints, and investigations of CPNI sales suggests that few customers were affected. Aside from evidence squarely to the contrary,[13] this argument contains a fundamental flaw--consumers cannot complain or sue, and government agencies cannot investigate, practices when they do not know that these practices are occurring. We can cite as an example the data breaches of sensitive information that occur on a disturbingly regular basis.[14] These events would not be heard of, and data protection would not be a household concern, had states like California not passed laws mandating notice to consumers of data breaches. The lack of complaints should therefore not be seen as the absence of a problem, but rather as an indictment of the extent to which consumers are kept in the dark as to the mishandling of their personal information.

Consumers' clear concern for their privacy would likely outweigh the inconvenience of not being able to instantaneously obtain another copy of their phone bill, contrary to the claims of many carriers.

Such claims seem even more farfetched when applied to consumers who would affirmatively place blocks on the disclosure of their CPNI. Verizon, for instance, makes the argument that a customer who places a "no-release" order on her information might then become frustrated if she is unable to obtain information on her own account.[15] The argument assumes that a person who has taken specific steps to prevent information disclosure would then be frustrated when the company follows those same steps.

Furthermore, Verizon assumes that such an order would be perpetual and prevent any disclosure whatsoever. This need not be the case, so long as the procedures and authentication methods for canceling the no-release order are far more stringent than current protections for CPNI disclosure.

---

[11] Comments of CTIA at 16.
[12] Comments of AT&T at 13.
[13] *See* n. 3-4, *supra*.
[14] Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the ChoicePoint Incident, http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[15] Comments of Verizon at 21, filed Apr. 28, 2006.

V. Opt-In

EPIC's earlier comments in this and other rulemakings address the need for an opt-in system for CPNI disclosures to joint venture partners and independent contractors, including the fact that such a system would be unlikely to infringe upon carriers' free speech rights under the First Amendment to the United States Constitution.[16] Here, we wish simply to make note of the fact that the same carriers who claim that notices to consumer will be ignored in the flood of information presented in billing statements rely upon this same deluge of fine print to notify their customers of their privacy rights.

VI. Data Limitation

EPIC has suggested that carriers should limit the amount of data collected from consumers to that which is strictly necessary to conduct business, and that data no longer useful for billing or business purposes be deleted or de-identified. Carriers have responded to this proposal by claiming that such deletion would frustrate billing purposes, harm marketing, and impede law enforcement.

EPIC's original petition suggested that call records should be deleted "after they are no longer needed for billing or dispute purposes."[17] By this very formulation, bills that are no longer likely to be in dispute, such as those that have been paid in full and not contested for some time, could be deleted with little loss of convenience for the customer, and a significant gain in privacy. Though carriers claim that pretexters are likely more interested in newer records, older records are still usable to establish calling patterns and to identify an individual's contacts over a period of time. In balance, the risk of disclosing that sensitive, even if dated, information could easily outweigh the risk that a consumer will need to request a bill she has paid for, and not disputed, several months ago.

Putting consumers' call records at risk for the benefit of the carriers' marketing departments, then, seems even less justifiable. In this context, it seems particularly disingenuous for AT&T to claim that its retention strategy benefits consumers because "many consumers appreciate targeted marketing."[18]

Carriers also note that current regulations require them to retain records for 18 months. However, the purpose for the storage in 47 C.F.R. 46.2 is discrete and limited: the provisions were enacted as a consumer protection measure to prevent "slamming," the illegal changing of a consumer's telephone service without permission. Data retained for the limited purpose of investigating slamming complaints should be used and disclosed only for that limited purpose. In order to fulfill this purpose and safeguard consumer privacy, EPIC recommends that the Commission amend the rules to allow for deletion

---

[16] *See, e.g.*, Comments of EPIC *et al.* at 13, filed Apr. 14, 2006.
[17] EPIC Petition, at 11-12, filed Aug. 30, 2005.
[18] Comments of AT&T, n. 21.

when the records are no longer necessary for assisting in the resolution of slamming disputes.

The Department of Justice also calls attention to the data preservation provisions of 18 U.S.C. § 415, which allow law enforcement to mandate the preservation of certain specific toll records. The major difference between such a data preservation scheme and a data retention scheme is that section 415 requires that, before information is stored for law enforcement use, the request is made pursuant to a judicial warrant. This requirement of individualized suspicion distinguishes the data preservation system of section 415 from a data retention scheme that captures all consumers' information wholesale.

VII. Safe Harbor

Verizon has raised the possibility of a "safe harbor" provision that would allow carriers to escape liability if they meet certain minimum standards.[19] While a clear set of secure baseline standards would, ideally, protect consumers, the specific provisions proposed by Verizon would not significantly increase the privacy or security of CPNI.

Verizon proposes six specific factors for a safe harbor rule: (1) cooperating with enforcement efforts, (2) participating in a working group to enhance security; (3) permitting customers to voluntarily apply passwords; (4) filing more detailed CPNI certifications; (5) posting privacy policies online; and (6) establishing categories of information, such as Social Security, driver's license, and taxpayer identification numbers, that should not be disclosed to residential customers.[20]

Though all of these goals are commendable, even taken all together, these steps do little to improve the security of consumers from the unauthorized CPNI disclosure that required this rulemaking. Cooperation with law enforcement efforts will not solve the systemic problem of poor security, for instance.

The most concrete of Verizon's proposals, prohibiting the disclosure of certain especially sensitive information, is a good practice, and one supported by other comments.[21] However, data such as Social Security numbers, credit card numbers and other elements of identity theft were not the data most immediately threatened by illegal CPNI disclosures. The data within CPNI that must be protected, and that the Verizon safe harbor fails to protect, is call information: who was called, when, and for how long. It is the possibility of tracing this information that raised the concerns of law enforcement, domestic violence prevention advocates, and ordinary consumers. If the Commission deems it necessary to implement a safe harbor provision, such a provision must be conditioned upon safeguards that provide real protection to consumers' call record information, and not unrelated data, no matter how sensitive.

---

[19] Comments of Verizon at 11, filed Apr. 28, 2006.
[20] *Id.*
[21] Comments of CTIA at 11.

VIII. Conclusion

Minimum standards for CPNI security are necessary to prevent the most egregious bad practices that made pretexting a viable business model for data brokers. The scope and seriousness of the problem require that the Commission take action to ensure that carriers provide real protection for consumers' CPNI.

Respectfully Submitted

Sherwin Siy
Staff Counsel
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
202-483-1140 ext. 110