Written Statement

of

Thomas J. Navin
Chief, Wireline Competition Bureau
Federal Communications Commission

Before the

Committee on Energy and Commerce
U.S. House of Representatives

On

"Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act"

March 9, 2007

Good morning, Chairman Dingell, Ranking Member Barton, and members of the Committee. I appreciate the opportunity to speak with you today about the ongoing work of the Federal Communications Commission to ensure the privacy of American consumers' sensitive telephone call records.

Section 222 of the Communications Act of 1934, as amended, requires telecommunications carriers to protect the confidentiality of their customers' personal information collected in the course of providing telephone service. This information is commonly referred to as customer proprietary network information or CPNI. As you are aware, third parties, known as "data brokers" and "pretexters," have invaded consumers' privacy by gaining unauthorized access to this very personal data for profit.

The Commission has taken several steps to curb the unauthorized disclosures and sale of consumers' personal telephone records. Specifically, FCC Chairman Martin has proposed imposing stricter security standards for CPNI for all providers of telephone service, including mandatory passwords for accessing customer call records. Further, the Commission has investigated, and will continue to investigate, this unlawful activity and take strong enforcement action to address any violations by telecommunications carriers of their obligations to protect CPNI.

Background

Congress enacted section 222 of the Act, as part of the Telecommunications Act of 1996 amendments, for the express purpose of protecting consumers' privacy. Specifically, section 222 of the Act provides that telecommunications carriers have a duty to protect the confidentiality of CPNI, which includes, among other things, customers'

calling activities and history, and billing records. The Act limits carriers' ability to use customer phone records even for their own marketing purposes without appropriate consumer approval and safeguards. Furthermore, unless otherwise required by law, the Act prohibits carriers from using, disclosing, or permitting access to this information without customer approval if the use or disclosure is not in connection with the service being provided. The Commission's rules also provide that a telecommunications carrier "must have an officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance" with the Commission's CPNI rules.

The Commission began its investigation of the data broker problem in late Summer 2005, and in August 2005, the Electronic Privacy Information Center ("EPIC") filed a petition for rulemaking to address the sufficiency of carrier privacy practices in light of the fact that online data brokers were selling consumers' private telephone data. As described in the petition, numerous websites were advertising the sale of personal telephone records, including records of calls to and from a particular phone number and the duration of such calls, for wireless and wireline customers. Following the filing of EPIC's petition, the Commission moved to consider rules that impose stricter security standards on all providers of telephone service concerning sensitive customer information. The Commission also took action to investigate these activities under the existing CPNI rules.

On February 1, 2006, Chairman Martin testified before this Committee and in response to a request by several members on how best to combat this problem, suggested

that Congress make illegal the commercial availability of consumers' phone records. In addition, Chairman Martin suggested that a more stringent "opt-in" approval method for protection of consumer phone record information could be implemented, and also proposed that Congress could strengthen the Commission's enforcement tools.

In the last session, Congress adopted legislation called the Telephone Records and Privacy Protection Act of 2006, which made pretexting a criminal offense subject to fines and imprisonment, and on January 12, 2007, the President signed this legislation.

On February 8, 2007, Chairman Dingell, Ranking Member Barton, and several members of the Committee introduced H.R. 936 to further prohibit fraudulent access to telephone records. I note that, among other things, the bill would make pretexting unlawful and would expressly extend "opt-in" approval requirements to the sharing of certain information with joint venture partners, independent contractors, and other third parties. Further, H.R. 936 would expand the penalties for CPNI violations and make it easier for the Commission to bring enforcement actions against non-common carriers, such as data brokers.

Commission Efforts to Strengthen Existing CPNI Rules

In response to the problem of pretexting, the Commission currently is considering new rules to ensure that carriers adequately protect their customers' private information. Specifically, the Commission issued a Notice of Proposed Rulemaking ("Notice") inviting comment on the EPIC petition and whether additional Commission rules are necessary to strengthen the carriers' safeguards for customer records.

Based on the evidence submitted in its rulemaking proceeding, and gathered in its enforcement investigations, the Commission learned that data brokers routinely seek to obtain unauthorized access to CPNI by impersonating an authorized user, the account holder or another company employee either when speaking with a carrier's customer service representative or via online access. There also has been evidence of some limited instances of employee misconduct. And while we consider it a positive development that numerous carriers (as well as the FTC and numerous states) have filed lawsuits seeking to enjoin pretexting activity, unfortunately it is also an indication of the success pretexters have had.

As we have met with parties regarding the strengthening of our CPNI rules and conducted investigations, we have learned of a variety of steps carriers can take to further protect the privacy of customer account information, some of which certain carriers are implementing today. These steps include, among other things, using better security and authentication measures in call centers and with respect to setting up online accounts; notifying customers of account changes; providing notice of unauthorized access to CPNI; and greater employee training and monitoring. Significantly, we also recognize the importance of this issue to law enforcement, particularly in light of the new Telephone Records and Privacy Protection Act of 2006, which makes pretexting a criminal offense.

The Commission has an item for consideration which would address these issues by requiring providers to adopt additional safeguards to protect customers' phone record information from unauthorized access and disclosure. The Chairman has circulated an order that, for example, proposes prohibiting providers from releasing call detail

information except when the customer provides a password, or by sending it to an address of record or calling the customer at the telephone of record. To protect against possible efforts to circumvent these requirements, the order proposes to require carriers to notify the customer immediately when information such as passwords or the address of record is created or changed. The Chairman also proposed a notification process for both law enforcement and customers in the event of a CPNI breach.

In addition, Chairman Martin proposed to modify our current rules to require providers to obtain affirmative customer consent before disclosing any of that customer's phone record information to a provider's joint venture partner or independent contractor for marketing purposes. Further, the order proposes to extend all CPNI obligations to interconnected voice over Internet protocol (VoIP) providers. These additional privacy safeguards should sharply limit pretexters' ability to obtain unauthorized access to CPNI.

Commission Enforcement Action

The Commission also has taken a hard look into the world of data brokerage and has used its enforcement authority against both data brokers and carriers to help address this problem. As a first step in its investigation and enforcement activities, the Commission issued subpoenas to several of the most prominent data brokers in late 2005, and again in 2006, seeking information about how companies obtained phone record information and then sold it. Some companies failed to respond adequately to our requests and almost all companies denied any knowledge of wrongdoing. As a consequence of the companies' failure to respond, the Commission issued letters of citation, and ultimately was forced to issue a Forfeiture Order against one company,

Locate Cell, for its continued failure to respond to the Commission's subpoenas. We also referred Locate Cell's inadequate response to the Department of Justice for enforcement of the subpoena.

Additionally, the Commission focused its attention on the telecommunications carriers' practices to fulfill section 222's duty to protect customer information. As a result of numerous meetings with various carriers, a review of the carriers' annual section 222 compliance certificates, and a review of the carriers' responses to formal Letters of Inquiry sent to nearly 20 carriers, the Commission issued three Notices of Apparent Liability for Forfeiture to carriers for failure to comply with the Commission's rules implementing section 222.

Throughout these investigations, the Commission closely coordinated with Federal Trade Commission staff. In addition, the Commission has offered assistance to state attorneys general in their efforts to combat pretexting.

Conclusion

The Commission takes very seriously any breach of consumers' privacy, as well as carriers' statutory duty to protect the customer information that they collect. The Commission also remains committed to strengthening its rules as warranted to help ensure that carriers implement adequate practices to protect their customers' privacy, as required by the Act. We likewise will continue to coordinate with the Federal Trade Commission, state and federal attorneys general, and other law enforcement authorities about our findings, and work with them in any way we can to take legal action against data brokers and pretexters. We look forward to working collaboratively with the

members of this Committee and other Members of Congress to ensure that consumers' personal phone data remains confidential. Thank you for the opportunity to testify, and I would be pleased to respond to your questions.