Written Statement of

Kris Anne Monteith
Chief, Enforcement Bureau
Federal Communications Commission

Hearing on
"Internet Data Brokers & Pretexting:
Who Has Access to Your Private Records?"

Before the
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives

September 29, 2006

Introduction

Good afternoon, Chairman Whitfield, Ranking Member Stupak, and members of the Subcommittee. I appreciate the opportunity to speak with you today about the ongoing investigations of the Federal Communications Commission into the issue of third parties' access to and sale of consumers' telephone call records. These third parties, also known as data brokers, use a variety of deceptive methods to obtain call detail and other personal information belonging to American consumers. Investigating how third parties obtain call records can provide critical information about the privacy practices employed by telecommunications carriers, over whom we have jurisdiction.

As FCC Chairman Kevin Martin stated in his testimony before the full Committee on Energy and Commerce in February 2006, the Commission is deeply concerned about the disclosure and sale of consumers' personal telephone records. The Commission has, and will continue to, take strong enforcement action to address any violations by telecommunications carriers of their obligations to protect customer proprietary network information ("CPNI"), as set forth in section 222 of the Communications Act of 1934, as amended, (the Act) and the Commission's rules.

Background

Numerous websites advertise the sale of personal telephone records for a price. Specifically, data brokers advertise the availability of mobile phone records, which include calls to and from a particular mobile phone number, the duration of such calls, and may even include the physical location of the mobile phone. In addition to selling mobile phone call records, many data brokers also advertise the sale of landline and voice over Internet protocol call records, as well as non-published phone numbers. In many cases, data brokers claim to be able to provide

this information within fairly quick time frames, ranging from a few hours to a few days. The data brokers provide no explanation on their websites of how they are able to obtain such personal consumer data. Discerning how they are able to do so is the focus of our inquiry, given the statutory obligations of telecommunications carriers to protect this data.

The mandate requiring telecommunications carriers to implement adequate safeguards to protect consumers' call records is found in section 222 of the Act. Congress enacted section 222 to protect consumers' privacy. Specifically, section 222 of the Act provides that telecommunications carriers must protect the confidentiality of customer proprietary network information. CPNI includes, among other things, customers' calling activities and history, and billing records. The Act limits carriers' abilities to use customer phone records even for their own marketing purposes without appropriate consumer approval and safeguards. Furthermore, the Act prohibits carriers from using, disclosing, or permitting access to this information without approval of the customer, or as otherwise required by law, if the use or disclosure is not in connection with the provided service.

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.

Commission Investigation

The Commission is currently taking a number of steps to investigate the unauthorized access to and sale of consumers' private phone records and to ensure that telecommunications carriers are fully meeting their obligations under the law to protect those records. First, we are investigating data brokers to determine how they are obtaining consumers' personal call records.

Second, we are investigating telecommunications carriers to determine whether they have implemented safeguards that are appropriate to secure the privacy of the personal and confidential data entrusted to them by American consumers. Third, the Commission has initiated a proceeding to determine what additional rules the Commission should adopt to further protect consumers' sensitive telephone record data from unauthorized disclosure.

The Commission began its investigation of the data broker problem in late Summer 2005, and, in November 2005, the Commission issued subpoenas to several of the most prominent data brokers. These subpoenas sought details regarding how the companies obtained phone record information and about the companies' sale of consumer call records. The companies failed to adequately respond to our requests. As a consequence, we issued letters of citation to these entities for failing to fully respond to a Commission order. In July 2006, we issued a Notice of Apparent Liability for Forfeiture against one of these companies, Locate Cell, for its continued failure to respond adequately to our subpoena. We also referred the inadequate response to the Department of Justice for enforcement of the subpoena.

In January 2006, we served another approximately 30 data brokers with subpoenas. We have reviewed and analyzed the responses received, and issued citations against companies that failed to respond fully to our subpoenas. In addition, in support of these investigations, we have made undercover purchases of phone records from various data brokers. This information has assisted us in targeting additional requests for information and in determining the exact method by which consumer phone record data is being disclosed.

In response to our subpoenas, the data brokers almost universally denied any knowledge of wrong doing, and claimed to be "middlemen" who just transmit requests for information to third parties. Although no company admitted to engaging in "pretexting," our investigations

reveal that data brokers routinely engage in this practice – often by impersonating the account holder or another company employee. Data brokers are also obtaining access to consumers' accounts online by overcoming carriers' data security protocols. And, we have seen some limited instances of employee misconduct – that is, employees of telecommunications carriers who illegally share this information with data brokers in exchange for a fee. Although pretexting is still taking place, we are pleased that in response to scrutiny from this Committee, the Commission, the Federal Trade Commission and other law enforcement authorities, as well as lawsuits brought by telephone companies, most of the data brokers that we originally subpoenaed no longer offer call records for sale.

In conjunction with our investigation of data brokers, the Commission has also focused its attention on the practices of the telecommunications carriers subject to section 222. The Commission's Enforcement Bureau staff has had numerous meetings with the major wireless and wireline providers to discuss efforts they have undertaken to protect their confidential customer data and to prevent data brokers from obtaining and using such information. Staff has probed into whom within the companies has access to call record information. Our discussions have also focused on the specific procedures employed to protect consumer call records from being accessed by anyone other than consumers themselves.

In January 2006, we issued a Public Notice requiring all telecommunications carriers to submit their most recent annual compliance certificate attesting that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. As a result of our investigation into carrier compliance with the annual certification requirement, we have issued three Notices of Apparent Liability for Forfeiture to carriers for their failure to

comply with these important rules. We have reached consent decrees, on this and other CPNI related issues, with two of these carriers totaling $650,000.

The Commission has also issued formal Letters of Inquiry (formal requests for information from carriers that may trigger penalties if not answered fully) to nearly twenty wireline and wireless carriers. These letters require the carriers to document their customer data security procedures and practices, identify security and disclosure problems, and address any changes they have made in response to the data broker issue. We have also issued supplemental Letters of Inquiry to the original nine largest carriers, and our in-depth analysis is ongoing.

Most recently, we issued Letters of Inquiry to a number of wireless and wireline carriers asking for information related to whether any CPNI of their customers was disclosed without authorization in connection with Hewlett Packard's activities.

During the course of our investigations we have learned that several carriers have taken a number of steps to further protect the privacy of consumer account information. These steps include, among other things: using better security and authentication measures with respect to setting up online accounts; notifying customers of password or account changes (i.e., wireless carriers will send a text message); and greater monitoring of employee activities to detect breaches in internal corporate policies.

Throughout our investigations, we have coordinated with the FTC whose jurisdiction is also implicated. Beginning last summer, Commission staff and FTC staff have been in regular contact regarding the sale of phone records by data brokers. Commission staff will continue to coordinate closely with the FTC staff and share with them any evidence of fraudulent behavior that we detect in the course of our investigation. The FCC has also responded to several inquiries and provided guidance to individual state Attorneys General, and the National

Association of Attorneys General (NAAG), as a number of states, including Florida, Illinois, and Missouri, take legal action against data brokers.

Commission's Efforts to Strengthen Existing CPNI Rules

In February 2006, the Commission adopted a Notice of Proposed Rulemaking granting a petition filed by the Electronic Privacy Information Center (EPIC) and inviting comment on whether additional Commission rules are necessary to strengthen the safeguards for customer records. Specifically, the Notice of Proposed Rulemaking seeks comment on EPIC's five proposals to address the unlawful and fraudulent release of CPNI: (1) consumer-set passwords; (2) audit trails; (3) encryption; (4) limiting data retention; and (5) notice procedures to the customer on release of CPNI data. In addition to these proposals, the Notice of Proposed Rulemaking also seeks comment on whether carriers should be required to report on the release of CPNI. Finally, the Notice of Proposed Rulemaking tentatively concludes that the Commission should require all telecommunications carriers to certify on a date certain each year that they have established operating procedures adequate to ensure compliance with the Commission's rules and file these certifications with the Commission.

The record in this proceeding closed in June. Chairman Martin has directed the staff to expeditiously prepare an order resolving the issues raised in the rulemaking proceeding and intends to bring an order before the full Commission for its consideration this Fall.

Conclusion

The disclosure of consumers' private calling records represents a significant invasion of personal privacy. The Commission is taking numerous steps to try to eliminate this troubling practice and give American consumers the privacy protections they expect. We look forward to

working collaboratively with the members of this Subcommittee, other Members of Congress, as well as our colleagues at the Federal Trade Commission and other law enforcement authorities 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.