



**Testimony of Elaine N. Lammert  
Deputy General Counsel, Investigative Law Branch  
Office of the General Counsel, Federal Bureau of Investigation  
before the U.S. House of Representatives  
Committee on Energy and Commerce,  
Subcommittee on Oversight and Investigations**

**June 22, 2006**

Good afternoon Mr. Chairman and members of the Subcommittee.

My name is Elaine Lammert and I am Deputy General Counsel of the FBI's Office of the General Counsel, Investigative Law Branch. I want to thank you for the opportunity to appear before you today to discuss the acquisition and sale of mobile phone records by online data brokers.

As the subcommittee is well aware, a significant number of online companies have openly advertised their ability to obtain and sell telephone call records. There are compelling reasons for the government to believe that these operations violate federal law. News accounts as well as expert testimony before Congress reflect that these records are most often obtained unlawfully through "pre-texting" or, in court room terms: fraud. Numerous data brokers are suspected of calling up phone companies and intentionally mis-identifying themselves and their purpose. By lying about their true identity -- perhaps by claiming that they are a fellow employee, or that they are the customer, or the customer's representative -- they manage to acquire statutorily protected information to which they have absolutely no right.

As you would expect, the FBI is actively investigating some of these practices as potential crimes, including potential violations of the wire fraud provisions of 18 U.S.C. § 1343. Under that statute, it is a felony -- punishable by up to 20 years in prison -- to falsely or under fraudulent pretenses obtain money or property by means of a wire communication in interstate or foreign commerce.

In addition, on May 3rd of this year, the Federal Trade Commission announced that it filed court complaints charging five Internet web-based operations with surreptitiously obtaining and selling confidential customer phone records without the customer's knowledge or authorization in violation of 15 U.S.C. § 45(a). The FTC, with the assistance of the Federal Communications Commission and a number of telephone companies, is seeking to stop these data brokers in their tracks and have them disgorge their unlawfully obtained proceeds. The privacy community also has raised concerns with the practices of these online data brokers.

It is fair then to say that the concern over how customer toll records are protected is widespread, and that protecting such records affects a wide array of interests. For example, similar to other individuals and businesses, law enforcement agencies also require that their call records be protected against unlawful disclosure. The FBI tested the ability of at least one online broker to gather information related to one of its own FBI telephone accounts, and the results were unacceptable: they obtained our records. It is easy to imagine how this type of data theft can negatively impact ongoing investigations, and therefore our ability to enforce the law and protect the country. And so, the FBI is interested in these activities both in terms of investigating possible violations of law and in order to protect the integrity of its own operations.

Of course, a range of laws already exist to protect the confidentiality of telephone

customer records. The Telecommunications Act of 1996 generally precludes telecommunications carriers from using, disclosing, or permitting access to "individually identifiable customer proprietary network information" except as required by law or with the approval of the customer. 47 U.S.C. 222(c)(1). The Electronic Communications Privacy Act ("ECPA"), codified at 18 U.S.C. §§ 2701-2712, also provides important rights for customers and subscribers of telephone companies, Internet Service Providers, and e-mail providers.

Under ECPA, for example, there are important restrictions on when a telephone company may voluntarily disclose customer records to the government. Pursuant to 18 U.S.C. § 2702(c), a telephone company may voluntarily provide the government with customer records only if it has the lawful consent of the customer or subscriber; as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the service provider; or, if the provider in good faith believes that an emergency involving danger of death or serious physical injury to any person justifies disclosure of the information without delay.

ECPA also describes in detail what information the government may require a company to provide when the government uses a warrant, subpoena or court order. As the statute relates to telephone toll records, 18 U.S.C. § 2703(c)(2) requires that -- in response to a subpoena -- a telephone company must provide the government with the relevant customer's name, address, local and long distance telephone connection records, length of service and types of services utilized, telephone or instrument number or other subscriber number or identity, and that customer's means and source of payment.

The FBI has significant interests in obtaining lawful access to telephone records in connection with investigations of all kinds -- including terrorism, espionage, drug trafficking,

child pornography, and more. In those cases, our practice is to strictly comply with ECPA. Indeed, it is part of the FBI's mission to prevent identity and information theft and to enforce the criminal laws designed to bring justice to those who do, or would, violate individual or business privacy.

I also wish to advise the Subcommittee that the Department of Justice has created a Privacy and Civil Liberties Board to ensure that Departmental programs and efforts adequately consider civil liberties and privacy. The Data Committee of the Privacy and Civil Liberties Board, on which the FBI is represented, was established earlier this year to address issues related to information privacy within the Department. Its first task is to respond to recommendations in the April 2006 GAO report entitled "Personal Information Agency and Reseller Adherence to Key Privacy Principles." The Data Committee members are analyzing the Department's use of all information reseller data, including internet data brokers, and will evaluate potential Department-wide policy with regard to such use. Specifically, all members of the committee are currently assessing their agencies' use of information reseller data, including the Internet data brokers identified by the Subcommittee as employing pretexting and fraud to obtain information. While the inquiry is ongoing, to this point, there is no evidence of widespread use of such services. The Data Committee meets on a monthly basis and expects to make recommendations to the Attorney General on this issue upon completion of its review.

Mr. Chairman and members of the subcommittee, the FBI fully supports the goal of protecting the privacy and security of customer telephone records from those who would acquire that information unlawfully. We are committed to enforcing the privacy and fraud laws aimed at achieving that goal. I thank you for your time today and would be happy to answer any questions.