

**Testimony of Edward Merlis,
Senior Vice President, Government and Regulatory Affairs
United States Telecom Association
Before the House Committee on Energy and Commerce
“Phone Records For Sale: Why Aren't Phone Records Safe From Pretexting?”**

February 1, 2006

Mr. Chairman, Ranking Member Dingell and members of the Committee, I am Edward Merlis, Senior Vice President, Government and Regulatory Affairs of the United States Telecom Association (USTelecom). On behalf of our more than 1,200 innovative member companies ranging from the smallest rural telecoms to some of the largest corporations in the U.S. economy, I want to thank you for this opportunity to testify on protecting consumers' phone records.

Our member companies offer a wide range of services across the communications landscape, including voice, video and data over local exchange, long distance, Internet and cable networks. We are united in our belief that it is time to update the nation's communications laws to reflect the dramatic technological and marketplace changes all consumers have witnessed in recent years.

This Committee has a long history of engagement in consumer protection and given Chairman Barton and Representative Markey's Co-Chairmanship of the Congressional Privacy Caucus, I know that the issue of safeguarding customer proprietary network information (CPNI) is of acute concern. I also appreciate the interest of Representatives Blackburn and Inslee in this issue and look forward to working with them as they move forward with their legislation.

USTelecom and all of its member companies share your concern for protecting customer information. Protecting the privacy of customer communications and records is an essential component of customer care by our companies and critical to the success of their businesses.

In today's intensely and increasingly competitive environment, carriers must take care of their customers if they are to succeed. The growth in the use of cell phones, email and text messaging has already reduced the number of wireline phone customers. Millions of customers have also switched their phone service over to those using Internet technologies. Our member companies cannot afford to take any customer and his or her confidential information lightly – or else they risk losing that consumer's business. As our companies attempt to offer video services, they stand little chance of successfully winning customers away from incumbent video providers – despite lower prices and enhanced services – if consumers cannot trust our member companies to safeguard their private information.

In addition to this strong business incentive to protect customers from potential harm caused by fraudulent operators, Section 222 of the Communications Act imposes a legal obligation as well. Telecommunications carriers have “a duty to protect the confidentiality of proprietary information of, and relating to, ... [their] customers.” This existing legal obligation is one taken very seriously by our member companies that have, in turn, devoted significant resources towards implementing a wide range of practices and procedures to safeguard the privacy of customer information. These practices include the education and training of customer service employees, implementation of security protocols and tightly defined agreements between our members and other businesses.

As Chairman Martin recently noted in his response to Representative Markey's inquiry, FCC rules already require "carrier[s] to certify annually that it has established operating procedures that are adequate to ensure compliance" with their Section 222 obligation, and "provide a statement explaining how [their] operating procedures ensure such compliance."

We believe the best way to address this problem is through the enforcement of existing laws and the strengthening of penalties on the bad actors who obtain information through unauthorized or fraudulent means. "Pretexters" are those who *pretend* to be the customer in order to gain access to protected records. By definition, these pretexters' activities would seemingly constitute an unfair or deceptive practice under Section 5 of the FTC Act.

Additionally, many of the so-called "data brokers," who use fraudulent methods or employ pretexters to obtain consumer information, are readily identifiable and should be subject to swift FTC enforcement. In fact, these brokers boldly advertise their purported ability to obtain confidential calling data. Any new rules related to this issue should focus on prohibiting bad actors rather than increasing the burdens on parties acting responsibly to protect consumer information.

While some have called for new mandated security measures, consideration and adoption of a new law must not give wrong-doers a roadmap to obtain confidential customer information. Moreover, it is highly likely that as soon as carriers implement specified, mandated security measures, crooks will quickly adapt their methods to circumvent new requirements identified in law or regulation.

As the Committee considers this issue, we would caution that new, specific security mandates also run the risk of adversely affecting consumers. Our member companies serve a diverse demographic background in terms of age, language, disability, and education, and they need the ability to develop specific solutions to meet their individual customers' needs. Imposing a one-size-fits-all requirement may unduly impede legitimate transactions between our member companies and their customers.

Mr. Chairman, we thank you for the opportunity to be here today. We look forward to working constructively with you and the members of the committee, to develop sound policies that focus on apprehending bad actors while not impeding the needs of our customers.

I look forward to responding to any questions you may have.

###