TESTIMONY OF
THE HONORABLE STEVE LARGENT
PRESIDENT AND CHIEF EXECUTIVE OFFICER
CTIA – THE WIRELESS ASSOCIATION®

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

MARCH 9, 2007

Good morning, Chairman Dingell, Ranking Member Barton, and members of the Committee. On behalf of CTIA, I am pleased to have this opportunity to testify on H.R. 936 and the steps that the wireless industry is taking to ensure the safety and security of wireless consumers.

At the outset, I want to be clear: CTIA's member companies take seriously their obligation to protect their customers' CPNI. In that sense, your goal is our goal too.

* * * * *

The Wireless Industry Is Committed to Protecting CPNI

Carriers have a duty to protect CPNI under the Commission's existing rules and Section 222 of the Communications Act. Beyond that, every carrier has a market-based interest in seeing that customer records are not disclosed without the proper permission. Any carrier which fails to adequately safeguard the privacy of its customers will -- and should -- suffer in the marketplace. For this reason, wireless carriers employ a broad range of security measures to prevent unauthorized access to and disclosure of these records. In general, the system works

well, as there are literally hundreds of millions of positive customer service interactions every year.

While it is the exceptions that generate headlines, I am pleased to tell you that since I last appeared before the Committee on this subject, much progress has been made to ensure that CPNI is protected, and that those who attempt to procure it illicitly are thwarted and punished.

Incidents like the unauthorized release of General Wesley Clark's call records and the Hewlett-Packard pretexting scandal served as a wake-up call for all of us. The wireless industry did not wait idly by for someone else to solve the problem. Each of CTIA's national carriers filed and obtained injunctions that shut down data thieves and the carriers teamed with law enforcement to identify individuals and companies involved in fraudulent activities to help put these criminals out of business.

CTIA supported legislation approved by the 109th Congress to criminalize the act of pretexting. President Bush signed the *Telephone Records and Privacy Protection Act of 2006* (H.R. 4709, P.L. 109-476) in January. Since enactment of that legislation, the market for pretexting services has evaporated under the threat of Federal prison time and sizeable financial penalties. The positive effect of the legislation cannot be overstated. Although the law is less than two months old, a Google search performed prior to this hearing did not find the kind of advertisements offering to procure customers' call records that were prevalent just a short time ago.

CTIA's members have not relied exclusively on the legal process to address pretexting.

In the past year, wireless carriers have adopted, and continue to adopt, a variety of procedures and tools to stop unauthorized access to CPNI. As is true in every other facet of the business, flexibility and innovation make a difference in the effort to thwart pretexting. This variation between carriers is a positive, as static practices can become outmoded or avoided by third parties with ill intent.

Some carriers have focused on process. Alltel, Cingular (now AT&T), and T-Mobile have implemented policies prohibiting their customer service representatives from providing call-detail information over the phone to anyone. Verizon Wireless has made a major commitment to enhanced training of customer service representatives. Others have chosen to use technology to help solve the problem. SprintNextel has embarked on an effort to utilize interactive voice response (IVR) technology to authenticate customers before the customer is routed to a customer service representative. IVR authentication can improve the security of customer accounts by further distancing authenticating information from customer service representatives, and by masking certain account information, such as call-detail records from the customer service representative, pending successful IVR authentication.

CTIA and its member companies strongly support additional enhanced security measures that can help to better protect consumers.

Specifically, CTIA supports giving customers the option of using passcodes. Many carriers already offer password protection, especially for online account access, for those customers who seek extra protection beyond the typical verification procedures. Across the wireless industry, passcodes have become standard operating procedure. Nonetheless, a blanket obligation that all accounts be password protected is undesirable, as passwords may not be wanted by every customer. Surveys and carrier experience have shown that some customers are burdened by having to remember numerous passwords for various accounts that may easily be forgotten or lost, and thus resist password protection for access to their account. In addition, there are customers who freely share their passwords with significant others and family members, therefore compromising the security of their own accounts. As an alternative to forcing password usage for all account access, CTIA supports a requirement that carriers make passwords available to all customers for account access. Customers should then be informed of the benefits of such passwords and the ways to effectively safeguard account access.

CTIA believes a rule that prohibits disclosure of a customer's entire Social Security Number, Tax ID, entire credit card number, or billing name and address in response to inbound customer calls may provide a useful deterrent to pretexting. There is no good reason why a carrier should provide customers with their personal-identifying account information. Many carriers already have implemented this procedure.

CTIA supports, and its carriers have adopted, policies that preclude the release of call detail records via fax or e-mail. Consumers seeking call detail information can only be provided

with that information if it is mailed to the address of record for billing purposes, or after the customer is called back on his or her registered mobile number. While some customers may find this practice inconvenient, this inconvenience is outweighed by the corresponding security benefits of these policies.

Finally, the Chair of the Federal Trade Commission, Deborah Majoras, has declared that the FTC has sufficient authority to act against parties that engage in the theft and illegal sale of call records. Nonetheless, if the Congress seeks to confirm the FTC's jurisdiction in this area, as is proposed in Title I of H.R. 936, CTIA would support such action, as we did last year. We would hope, however, that providing the FTC with civil enforcement authority will not in any way diminish the criminal prosecution of data thieves.

Wireless Carrier Concerns with H.R. 936

While CTIA supports reasonable measures to enhance the security of CPNI, CTIA's members have strong concerns about "one size fits all" legislative proposals that do not provide carriers with the flexibility that has served them so well in the marketplace. Any legislative obligations the Committee proposes should be narrowly targeted and responsive only to actual problems rather than theoretical possibilities and provide the flexibility that carriers need to innovate and compete. With this in mind, I have several specific observations to offer.

First, CTIA's members are concerned about any provisions in H.R. 936 that would require carriers to obtain specific customer consent – whether "opt-in" or "opt-out" – before they can

share CPNI with affiliates and joint venture partners that provide marketing and other services to carriers that are otherwise permissible under the law.

In instances where CTIA member companies share CPNI with third parties to aid in marketing, billing, and customer service efforts, they impose strict contractual obligations to protect customer information. There are also existing FCC requirements that cover such arrangements.

Additionally, the imposition of new restrictions on the ability of carriers to share CPNI with joint venture partners or independent contractors is unduly burdensome and has no connection with the goal of preventing fraudulent access to phone records. Many CTIA members employ third-parties to assist with billing and customer care functions. The parties that engaged in these activities for our carriers are bound by strict safeguarding agreements that govern both confidentiality and security obligations.

In general, industry practice obligates subcontractors to (1) use administrative, technical, and physical safeguards to protect customer information, (2) access and use customer information only on a need-to-know basis, (3) maintain strict confidentiality of customer information, (4) return or destroy customer information when it is no longer needed, and (5) submit to security and privacy audits. Contractors generally work in highly controlled environments and handle information that, while technically considered CPNI, is not the call-detail CPNI that pretexters seek.

CTIA is not aware of any credible suggestion that third-party contractors or joint venture partners have misused any CPNI that has been shared with them by a wireless carrier. The national carriers and Tier II carriers such as U.S. Cellular Corp., Dobson Communications, and MetroPCS Communications have each noted in their FCC filings that restricting or imposing burdensome requirements on the use of independent contractors and joint venture partners to help deliver, bill for, and market products and services to consumers will raise costs without any corresponding benefit. This problem might be particularly acute for smaller carriers which lack the ability to spread potential compliance costs over a national customer base.

While the bill appears to permit some sharing of information with third parties to initiate, render, bill, and collect for services and to provide customer service, this exemption is potentially compromised by the sweeping restrictions on disclosures elsewhere in the bill. We believe that an approach focused on enhanced security rather than introducing additional customer consent mechanisms is the most effective, cost-beneficial, and constitutionally permissible means by which to protect CPNI.

As a general matter, wireless companies should have the flexibility to use CPNI to market services other than telecommunications and Internet access to customers whose prior purchasing habits suggest they may be interested in additional services. Amazon.com and L.L. Bean have that flexibility; wireless carriers should too. Wireless carriers do not safeguard CPNI any less when such information is used to market other services as compared to when it is used to market their core services, and, as the record in the FCC's proceeding on

the EPIC petition demonstrates, there is no causal connection between Section 222's existing "opt-out" regime and the fraud perpetrated by pretexters. Depriving wireless carriers of the ability to use CPNI to market additional services to existing customers is not a necessary part of the effort to eliminate pretexting.

Unfortunately, as drafted, the bill appears to preclude a wireless carrier from informing only that subset of customers who have handsets that can receive a new service such as mobile TV (e.g., Verizon Wireless' V-Cast or Qualcomm's Media Flo) that such services are available. Instead, a carrier wishing to offer these services would have to market them to its entire customer base – in some cases as many as 50 million people – just to reach early adopters. This is a terribly inefficient restriction on a competitive business, and it does not make CPNI any safer.

CTIA also opposes the provisions of H.R. 936 that direct the Commission to consider whether it should require carriers to encrypt all stored CPNI data. The Commission is already considering such a requirement in its current proceeding, and thus far the record shows no evidence of unauthorized access of stored CPNI within carriers' databases. Mandatory encryption of stored call records would not have the effect of preventing pretexting. Conversely, it would increase costs, potentially delay response to legitimate customer service inquiries, and needlessly complicate carrier storage and access methods. Accordingly, CTIA urges that this provision be dropped from the bill.

In addition, the bill's provisions on "Access to Wireless Telephone Numbers" are overly broad. I appreciate what the drafters of this language were attempting to achieve when it was added to the bill last year, and I can assure you that CTIA's member companies have no plans to create a wireless directory without a customer's express opt-in consent. However, wireless numbers are employed for other important and legitimate uses -- such as the sale and delivery of third-party content, including things like news alerts, games, and ring tones -- that should not be frustrated by efforts to limit the creation of a directory.

Finally, if Congress opts to act in this area, it should do so in a way that promotes uniformity and efficiency. We are seeing increased attention being paid to these issues at the state level, where at last count, 34 different pieces of legislation (in 17 states) related to call records have been introduced this year. In the last legislative session, there were 75 bills in 28 states. Even when these bills are generally alike, they often contain variances that can make them difficult and costly to implement. The wireless industry does not welcome having to deal with a multitude of varying state-by-state obligations in this area. How well a consumer is protected, or what obligations a carrier faces, should not vary widely by location, and what is needed is a uniform national policy that properly balances the need to protect consumers while allowing carriers the flexibility to operate in the most efficient and cost-effective manner possible.

* * * * *

I believe that the wireless industry is in a better place today than the last time I appeared before you on this subject. The carriers have invested significant time and resources to make CPNI more secure. The much-publicized criminal activity that prompted congressional attention led to enactment of important legislation that dried up the market for pretexting. Equally importantly, these actions have focused the industry on efforts to improve its practices. Real progress is being made, both in terms of employee training and investment in new and improved systems, and that commitment will continue.

I commend the Committee and the authors of this legislation for the attention you have focused on this issue. The wireless industry looks forward to continuing to work with you to ensure that our customers' phone records are protected. I do hope, however, that as the Committee considers H.R. 936, you will preserve the wireless industry's flexibility to continue to provide consumers with innovative new services at affordable prices.

Thank you for the opportunity to share the wireless industry's views on this matter.