

August 22, 2011

The Honorable Mary Bono Mack
104 Cannon House Office Building
Washington, D.C. 20515

Dear Congresswoman Bono Mack:

On behalf of CTIA – The Wireless Association® (“CTIA”) and our members, thank you for the opportunity to respond to your inquiry of July 18. CTIA appreciates this chance to share the wireless industry’s view on how American consumers can avoid becoming vulnerable to the sort of intrusions that appear to have occurred in the United Kingdom. As detailed in our answers to your specific questions, it is our view that there are sufficient safeguards in place to prevent similar privacy breaches here in the United States.

1. As communications through voice over internet protocol (VOIP), smartphones and other mobile devices become more integrated in our daily lives, do you expect to see a rise in phone hacking here in the United States (involving both personal conversations and voicemails) as criminals search for new ways to steal valuable information such as credit card numbers, bank account numbers, Social Security numbers and biometric identifiers?

While it is not possible to attest to the contents of the average voicemail in-box, CTIA does not see voicemail as a likely source for criminals to obtain credit card or bank account information, social security numbers or biometric identifiers. Financial institutions, medical companies, and other regulated entities are subject to sector-specific privacy requirements that prohibit or discourage leaving sensitive information on voicemail.

The wireless industry is committed to protecting the personal information of wireless users. CTIA’s carrier members use a variety of methods to protect users, including technological solutions employed at both the network and device levels, and education of consumers about best practices that can be used to safeguard information.

2. At present, what safeguards do your member companies employ to ensure that American consumers are adequately protected against the type of phone hacking scandal currently being investigated in the United Kingdom?

There is a difference between “hacking” and the events that are under investigation in the United Kingdom. Hacking generally involves an assault on a

protected system or systems. The events that appear to have occurred in the United Kingdom seem to have stemmed from non-technical intrusions through which individuals took advantage of default or non-existent voicemail passcodes or PINs to obtain information from individuals' voicemail accounts. This would be more difficult to accomplish in the United States, since U.S. carriers require their customers to establish PINs to authenticate access to voicemail services, although some companies, as an optional convenience often chosen by consumers, do not require users to enter their PINs when they are calling voicemail from their own telephone numbers.

3. In the wake of this scandal, do your member companies believe it is necessary to adopt new practices to ensure that consumers in the United States are better protected in the future?

We believe that the current legal framework that applies to carriers and existing carrier practices are sufficient. Additional action may be necessary, however, to ensure that would-be hackers cannot easily obtain access to "spoofing" software that facilitates their ability to engage in criminal activity and appears to have few legitimate uses. The recent Federal Communications Commission ("FCC") order implementing rules adopted pursuant to the Truth in Caller ID Act (47 U.S.C. 227(e)) contained discussion on this point. See *In the Matter of Rules and Regulations Implementing the Truth in Caller ID Act*, WC Docket 11-39, adopted June 20, 2011, at paras. 37-42.

4. Do you believe existing laws and regulations adequately protect consumers in the United States from phone hacking and similar privacy breaches?

Yes. Although it is perhaps not possible to eradicate efforts to obtain unauthorized access to users' voicemail, this is not because the existing legal framework is inadequate. Under the Telephone Records and Privacy Protection Act, 18 U.S.C. 1039, it is illegal to obtain, attempt to obtain, or transfer confidential phone record information through misrepresentation or improper access without prior authorization from a customer. Similarly, the Stored Communications Act, 18 U.S.C. 2701, prohibits unauthorized access to stored electronic communications. Under the Wiretap Act, 18 U.S.C. 2511, it is illegal to obtain, disclose or use (or attempt to obtain, disclose or use) the contents of an intercepted wire, oral or electronic communication. Finally, under the Truth in Caller ID Act, it is unlawful to "knowingly transmit misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value."

In addition to these statutory limitations, the FCC prohibits wireless carriers from releasing customer information to customers who call the carrier except when the customer provides a password. If the customer does not provide a password, the

wireless carrier may not release customer information except by sending it to the customer at the address of record or by calling or texting the customer. Wireless carriers also must provide password protection for online customer accounts, and carriers must notify customers immediately when a customer creates or changes a password, a back-up for a forgotten password, an on-line account or an address of record. Finally, the FCC requires wireless carriers to report to their customers and law enforcement officials such as the Federal Bureau of Investigation if any customer information is disclosed without permission. And the FCC requires carriers to take reasonable measures to discover and protect against pretexting.

5. Approximately how many phone hacking incidents are reported by your member companies in a year? Are the number of incidents growing or declining?

An informal survey of CTIA's carrier members suggests that they receive either none or very few reports of phone hacking incidents and carriers do not report experiencing any sort of near-term increase in these incidents.

6. As a matter of practice, are phone hacking incidents, or suspected incidents, reported to law enforcement agencies and regulatory agencies?

To the extent that carriers are made aware of instances in which a crime is known or suspected to have occurred, some carriers contact law enforcement and regulatory authorities directly, while others recommend that the customer do so.

7. From a technological standpoint, how difficult is it to hack into cell phones or other mobile devices?

If the device is protected by a customer-generated passcode, it is not easy to break into a cell phone or other mobile device. In the absence of a passcode or PIN, it may be possible to access a voicemail account using Caller ID spoofing services that make it appear that a call is being placed from the subscriber's phone when it is not. Use of spoofing services for this purpose, however, is against the law, as it would fall within the scope of activities covered by the Truth in Caller ID Act and the Federal Communications Commission's rules implementing that measure.

8. What steps can consumers take on their own to better protect their personally identifiable information when communicating through either fixed wire or wireless devices?

Customers who minimize their risk become harder targets for criminals. Carriers recommend the use of passcodes, PINs, and application locks that are either provided by the carriers or are available in the third-party application market. Carriers also take steps, at the point of sale and on-line, to educate consumers about the tools that are available to promote the secure use of wireless services and

devices. Ultimately, however, it is up to consumers to educate themselves and make use of these tools.

I hope these responses address your concerns. I believe that current carrier practices and the strong legal framework already in place are sufficient to protect consumers, especially when consumers take an active role in using the security options the wireless market makes available to them. Nonetheless, CTIA would be pleased to work with you and your staff to address any additional concerns you may have.

Sincerely,



Steve Largent