



August 22, 2011

Chairman Mary Bono Mack
104 Cannon House Office Building
Washington, DC 20515

Dear Chairman Bono Mack:

The Information Technology Industry Council (ITI) is pleased to provide the following response to your letter on July 18, 2011, on the United Kingdom's phone hacking scandal and the possible repercussions in the United States.

ITI is the premier voice, advocate, and thought leader for the information and communications technology (ICT) industry. ITI's 50 members comprise the world's leading technology companies. As both producers and consumers of security products and services, our members have extensive experience working with the U.S. Government—as well as governments around the world—on the critical issue of security policy. As you are aware, the interests of industry and governments in increasing security are fundamentally aligned.

You are right to point out that the scandal has occurred in the UK, and so far no evidence has arisen to suggest such practices took place in the U.S. by the media. We must also point out that in the UK, the anger over the scandal has been justifiably directed at the press, the police and politicians. There is a consensus that technology companies are in no way responsible for these heinous practices. Nevertheless, before responding directly to your questions, we believe it is important to understand how the hacking occurred.

It is important to note that by "hacking", we are referring to the unauthorized access of a user's voicemail. In the case of the UK scandal, this was done in three ways. The first way is simply by calling a phone from two other phones at the same time, sending one caller to voicemail. That caller then enters the code number to retrieve voicemail remotely. Hackers depend on the fact that many people never change the default PIN for voicemail retrieval. The default PIN is typically a code such as 1111, 0000 or 1234 to enable customers to use their voicemail from day one. Customers are repeatedly told by service providers to change their voicemail PIN on a regular basis, but unfortunately very few do this. The second way that voicemails were accessed involved the hackers contacting the user's service provider and posing as the user to gain his/her security code.

Chair: Pamela Passman, Microsoft • Vice Chair: Peter Cleveland, Intel •

Officers: Dean C. Garfield, President and CEO • Ralph Hellmann, Senior Vice President • John Neuffer, Vice President for Global Policy
• Rick Goss, Vice President for Environment and Sustainability



The third way that voicemails were accessed involves a method called “spoofing,” whereby the hacker makes it appear as though he/she is calling from the phone that he/she wishes to break into. If a customer dials their own number from their own cell phone, they are typically directed to their own voicemail. For convenience, many service providers do not require a PIN if the customer is seen to be dialing from their own phone and even if they do, as previously mentioned, many customers do not take this precaution. Consequently, a hacker can easily gain access to a customer’s voicemail through spoofing the number transmitted to the voicemail service.

It is worth underscoring the fact that the voicemail service is not a physical part of any cell phone apparatus, and therefore is not stored on a cell phone in any tangible sense. Voicemail is stored on the server of the user’s service provider and the cell phone device merely enables a user to access the voicemail.

- 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 and Social Security numbers?*

The phone hacking in the UK involved accessing the voicemail of specific users. Currently, we do not believe it is common practice for valuable information such as credit card numbers, bank account numbers and social security numbers to be conveyed in voicemail messages and we certainly do not advise that users keep confidential information of that nature on the voicemail of their cell phones. Similarly, we believe that best practices mean that banks, government institutions and other organizations that hold confidential information do not typically relay said information in voicemail messages. We hope that this would continue and that the UK phone hacking scandal remains an isolated case.

- 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?*

ITI’s member companies have encouraged users to keep their voicemail secure by using a secret PIN that is known only to authorized users. Our members have encouraged users to regularly reset these voicemail PINs and to make the PIN something that is not easy to guess – such as a date of birth or consecutive string of numbers - thus treating voicemail security with the same gravity as they would other passwords and security codes for banking, emails, etc. ITI member companies also advise users to regularly delete voicemail messages, not just for storage reasons, as our technology companies are cognizant of the security benefit of such an action.



Furthermore, we must note that many of the incidents of phone hacking in the UK took place several years ago. Indeed, the hacking of Milly Dowler's phone, which served as the catalyst for public outrage in the UK case, occurred in 2002. Naturally, security has undergone huge improvements and many of ITI's member companies have launched smartphones that have advanced security in all areas, especially voicemail.

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?*

ITI's member companies have led the way in technological innovation and have taken huge steps to improve security. Nonetheless, we must understand that security is not an end state. It is a means of ensuring that the benefits from the digital infrastructure continue to grow. No sector of the economy, whether offline or online, is – or can ever be – 100% secure and without some inherent risk. In any case, the breach did not emanate from cell phone devices, but rather from voicemail, which is stored by service providers on their servers.

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

ITI's member companies have always endeavored to protect users from privacy breaches. Therefore, we were alarmed to see that some of the breaches that occurred in the UK involved payment to police officers for telephone numbers and to procure phone-tracking data. ITI has always been concerned about the rules around government access to confidential consumer information and how the government and its authorities use this data. The UK case highlights that great care must be taken when designing legislation that involves access to consumers' personal information.

Furthermore, we must note that in the U.S. legislation already exists to deal with spoofing. The Truth in Caller ID Act, which was signed into law in Dec. 22, 2010, prohibits caller ID spoofing for the purposes of defrauding or otherwise causing harm. In June 2010, the Federal Communications Commission (FCC) adopted rules implementing the Truth in Caller ID Act. The FCC's rules "prohibit any person or entity for transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value." Similarly, the Gramm-Leach-Bliley Act makes it illegal to access personal information under false pretences, and in 2007 the FCC strengthened the laws to prevent pretexting (the practice of obtaining someone's personal information under false pretenses), requiring telephone and wireless carriers to adopt additional safeguards to protect the personal telephone records of consumers from unauthorized disclosure.



The government can protect consumers through enforcement of existing laws, and additional legislation would not prove to be a panacea for breaches. Indeed, in the UK it is a crime to intercept phone calls without judicial authorization, but this did not stop the hackers from carrying out their actions.

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

As device manufacturers, ITI's member companies do not hold any information on phone hacking. Such information would be held by the service provider given that it is service providers that are hacked to gain access to voicemail messages, not mobile devices.

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

ITI member companies manufacture cell phone devices and do not have access to any information on phone hacking or similar incidents. We are therefore not in a position to record such occurrences. Service providers are in charge of running cell phone networks and are consequently the only entity could hold information on phone hacking incidents.

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

We advise that consumers take the requisite security measures to prevent occurrences of hacking. As previously stated, ITI's member companies have always educated their customers so that they can protect themselves from data breaches. Consumers should always take advantage of the tools at their disposal.

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?*

Aside from the steps we already mentioned, such as utilizing your voicemail PIN, we believe that better awareness is the key to improving security. Many users do not adequately utilize the range of tools available to them. Therefore, the public and private sector should continue to bolster outreach campaigns by educating members of the public on cell phone security issues through awareness videos, commercials, and free help.



Information Technology Industry Council

Leading Policy for the Innovation Economy

We hope that our responses to the questions raised in your letter are helpful and will receive due consideration. We are available at any time to elaborate on our comments and our responses. ITI and its members look forward to continuing to work with your office on these and other important issues affecting the ICT industry.

Thank you very much for your consideration.

Sincerely,

Dean C. Garfield
President and CEO
Information Technology Industry Council (ITI)