



WALTER B. MCCORMICK, JR.  
President and Chief Executive Officer

August 5, 2011

The Honorable Mary Bono Mack  
Chair, Subcommittee on Commerce,  
Manufacturing and Trade  
2125 Rayburn House Office Building  
U.S. House of Representatives  
Washington, DC 20515

Dear Chair Bono Mack:

Thank you for your letter of July 18, 2011, concerning the recent phone hacking and police bribery scandal unfolding in the United Kingdom. On behalf of the United States Telecom Association, I am pleased to respond to your timely inquiry.

Your letter seeks reassurance from our industry that safeguards exist to prevent similar privacy breaches from occurring in the United States. Let me begin by providing those assurances to you on behalf of the wireline voice and broadband industry. Our companies' security policies and best practices, protections built into communications devices and services, legal protections and prohibitions, and consumer education and offerings designed to mitigate against intrusions such as those alleged to have occurred in Britain, make the odds of success very small indeed for any similar effort aimed at our customers here in the United States.

It may be useful to begin a fuller discussion of this issue by pointing out that the term "hacking" itself means different things to different people. Engineers would suggest that hacking, in the literal sense, requires an intrusion into a system otherwise believed to be protected by a variety of technical barriers to that intrusion. By contrast, what the media has characterized as a "hacking" scandal in the United Kingdom in point of fact appears to involve efforts at successfully accessing individuals' voice mails because those individuals or their service providers relied on weak or even absent barriers to such intrusion.

Moreover, the British experience, at least in this instance, appears to involve only mobile devices. By contrast, our member companies take extraordinary measures to secure not only their wireline, wireless, and broadband networks in the United States, but also their Internet networks that enable global communications. American laws, including the Telephone Records and Privacy Protection Act, 18 U.S.C. 1039; the Stored Communications Act, 18 U.S.C. 2701; and the Wiretap Act, 18 U.S.C. 2511, also provide additional consumer privacy protections. As a practical matter, intercepting conversations or voice mails occurring on our Nation's wireline communications

August 5, 2011

Page 2

networks is considerably more difficult than the kind of nontechnical intrusions reported in the UK scandal. Indeed, we are aware of no reports of such unlawful interceptions occurring on the wireline networks of our member companies.

Our member companies work extremely hard to operate their networks in full compliance with federal law in order to protect the privacy of their customers. However, there have been instances of illegal call interception reported on unprotected VoIP networks. It is important that any law be applied uniformly to all, regardless of the type of technology used or business a particular company is in.

For example, while Caller ID technology has long enabled a called party to learn who is calling his or her phone, a tactic called “spoofing” regrettably enables some callers to lie about their identities and present false names and numbers that in turn can be used as a tool to defraud, harass, or spy on others. In the British situation, it appears that third parties were able to obtain the cell phone numbers of consumers and then to use Caller ID spoofing services to dial into those consumers’ voice mail accounts where passcodes were weak or nonexistent.

In the absence of strong passcode protections built into networks and devices – something that unfortunately appears to have been a common problem in the UK – wrongdoers were able to gain access to the voice mail messages left on those consumers’ cell phones. By contrast, American consumers are generally provided with and encouraged by their providers to use tools and services that provide greater assurance of security for their personal information, including strong passcodes, locking features, and encryption applications for the data on their cell phones and other devices.

Of course, as we know from long experience, certain criminal elements in our society will always attempt to exploit weaknesses in any system for some sort of material or other gain. Thus, our member companies devote enormous resources to trying to remain one step ahead of those wrongdoers. We hope that law enforcement authorities are doing the same. Like you, our industry appreciates the importance consumers place on the privacy of their voice communications, and we will continue to adopt and implement policies, procedures, and practices that minimize the chances that our customers’ privacy will be unlawfully compromised.

Sincerely,



Walter B. McCormick, Jr.