



**Consumer Electronics Association**  
1919 South Eads Street  
Arlington, VA  
22202 USA  
866-858-1555 toll free  
703-907-7600 main  
703-907-7601 fax  
CE.org

August 22, 2011

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

Dear Congresswoman Bono Mack:

Thank you for your inquiry regarding the ongoing phone hacking scandal in the United Kingdom and its implications for consumers in the United States.

The Consumer Electronics Association (CEA) is the preeminent trade association representing the consumer electronics industry. Our 2,000 member companies include the most innovative companies in the United States, such as device manufacturers, service providers, and both small and large retailers.

CEA appreciates your continued work to protect the privacy and financial assets of our fellow citizens and you raise important issues. Please find our responses to your July 18, 2011 letter below:

- 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?*

It is difficult to provide a specific answer to this question as we are unaware of current rates of phone hacking in the United States and unsuited to predict the future actions of criminals and/or other bad actors. Nonetheless it seems unlikely that criminals would seek to access mobile device and VOIP voicemail boxes in order to obtain credit card numbers, bank accounts and Social Security numbers simply because this sort of sensitive personal information is unlikely to be stored on wireless devices.

The rapid shift to commercial transactions with wireless devices may give rise to creative crimes. Bonnie and Clyde robbed banks because that's where the money was. Increasingly, financial transactions are in digital signals and transmitted through wireless smart phones. However, landline phones and the Internet have been used for some time for financial transactions and they have been used as a media for fraud just as any new technology can be expected to be used for legitimate and illegitimate purposes. The advantage of newer technologies is that they offer access, portability, efficiencies and new uses. The disadvantage is that new technologies can also be used illicitly. Fortunately the regimen to limit consumer liability for credit card information misuse (\$50 maximum

liability) Congress enacted four decades ago still protects consumers. Bank account numbers and access to the accounts may be more problematic.

Phone hacking of wireless devices whereby someone monitors the call to gather financial or private information in the United States seems to be rare to non-existent outside of authorized government action. But deep packet inspection of wired and wireless information when Internet Protocol (IP) is being used is increasingly common by carriers seeking to limit massive spam from unapproved sources. More, content owners increasingly are demanding the right to inspect all IP transmissions to determine if copyrighted content is being transmitted without authorization and seeking a private right to do so. To the extent Congress and government agencies authorize deep packet inspection, especially to commercial interests, there is more potential for mischief. Indeed, the American Constitutional philosophy of protecting citizens from their own government, rather than the European approach of massive ambiguous laws regulating business activity, remains the approach which is more innovation-friendly. In other words, the potential harm here of regulation and government involvement can have unintended consequences, especially as we see no evidence of a problem and thus would urge caution in legislating.

- 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?*

The phone hacking scandal currently under investigation in the United Kingdom concerns the accessing of mobile device voicemails. Mobile device voicemail services are provided by the mobile service provider and are outside the control of device manufacturers. It is our understanding that mobile service providers instruct their customers on how to password protect access to their voicemail accounts.

- 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?*

From what is now known the phone hacking incidents currently under investigation in the United Kingdom, it appears that these occurrences are attributable to a unique and coordinated series of illegal acts rather than a breach of mobile device technological safeguards.

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

Yes it appears so, but with two caveats noted below.

The following laws provide a strong deterrent to phone hacking and unauthorized access to voicemail messages:

18 U.S.C. 1039

(Telephone Records and Privacy Protection Act of 2006)

Strengthens protections for law enforcement officers and the public by providing criminal penalties for the fraudulent acquisition or unauthorized disclosure of phone records.

18 U.S.C. 2701

(Stored Communications Act (enacted as part of the Electronic Communications Privacy Act of 1986))

Provides criminal penalties for anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided or... intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system."

18 U.S.C. §2511

(Wiretap Act)

Prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies.

47 U.S.C. 227

(Truth in Caller ID Act of 2009)

Amends the Communications Act of 1934 to make it unlawful for any person in the United States, in connection with any telecommunications service or Internet protocol (IP)-enabled voice service, to cause any caller identification (ID) service to transmit misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted in connection with: authorized activities of law enforcement agencies; or a court order specifically authorizing the use of caller ID manipulation.

These laws protect consumers by making all forms of hacking illegal. One caveat is that technology is always evolving, criminals are creative and courts are not always consistent, so we should monitor developments and see if bad behavior slips through legal cracks.

While these laws discourage behavior, consumers are already well-protected against misuse of their credit cards through the limitation of their liability to \$50.

The other caveat is that while we are not experts in this area, bank deposits, including money with brokerage houses and even stocks, bonds and other financial instruments in electronic form are not similarly protected. While we are not suggesting an analogous protection limiting consumer liability to \$50, we wonder if financial institutions should be encouraged or even required to give consumers the option of requiring a secondary form of approval for major extraordinary transactions. This is less a technology issue and more a common sense approach. Using a found cell phone at Starbucks to buy coffee is not an issue for Congress, but using it to wipe out a bank account may be.

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 noted previously, mobile device voicemail services are provided by mobile service providers and are outside the control of device manufacturers. CEA device manufacturer members are therefore unsuited to comment on this question. Phone hacking has been off our radar, and has not been discussed since the early days of cordless phones when occasionally the earliest primitive models may have shared the same frequency (similarly in the first generation of products, you could occasionally open your neighbors' garage doors or unlock their cars with your remote or keyless entry). In almost every case, these issues are resolved with more elegant security. In the case of phones, computers, and other technologies (including cars), if someone accesses your security

information (or key) they can have access. Biometrics as a security block will trend upward if hacking and theft increase. This has costs in time and money, but the technology is improving and it is definitely a trend in facility and border security and for those that want it, computer security.

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

We do not know. None have been reported to us by our retail and device makers nor has this been discussed as a problem in any CEA meeting in over three decades to my recollection.

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

Mobile device voicemail services are provided by mobile service providers and are outside the control of device manufacturers and retailers. CEA device manufacturer members and retailers are not suited to comment on this question. Nonetheless, CEA and its members strongly believe that the use of pass codes by consumers to access their voicemail accounts is essential to protecting against unauthorized access. As to non-voice mail hacking, please see answers above.

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?*

CEA recommends that consumers use the tools and advice provided as part of their mobile service contracts, which includes information on how to establish and use voicemail pass codes.

We appreciate your commitment to safeguarding the privacy and security of American consumers and we look forward to working closely with you on this critical issue. If we can provide you with any additional information, please don't hesitate to contact me at 703-907-1515 or gshapiro@ce.org.

Sincerely,



**GARY SHAPIRO**  
President & CEO