LG ELECTRONICS USA, INC.

1000 Sylvan Avenue
Englewood Cliffs, NJ 07632

April 11, 2012

The Honorable Henry A. Waxman, Ranking Member
The Honorable Anna G. Eshoo, Ranking Member –
Subcommittee on Communications and Technology
The Honorable Edward J. Markey

Dear Representatives Waxman, Eshoo and Markey:

On behalf of LG Electronics USA, I am pleased to respond to your March 23 letter addressed to Mr. Bon Joon Koo in which you asked a series of questions regarding LG's policies related to cell phone security. As demonstrated in the replies below, LG is very committed to protecting the users of our electronic equipment. LG has developed policies and guidelines to help ensure that consumers' utilization of our equipment is secure, and to deter misuse or theft.

Below are our company's specific responses to your inquiries.

1. **What company policies and guidelines do you currently have in place that relate to cell phone theft or loss?**

   Currently, all Android smartphones manufactured by LG can be password protected by the consumer, either at start-up or any time thereafter. Password protecting a phone prevents someone from getting past the locked screen of a lost or stolen device without entering the applicable passcode and thus prevents access to the device rendering it inoperable. LG includes instructions in our phone manuals on how to do this. We believe password protection is a simple and yet effective tool for consumers to utilize right now to help prevent unauthorized access to a lost or stolen device. We are also aware of a number of third-party applications currently available for download on the Android Market that advertise themselves as being capable of remotely wiping a mobile phone after it is lost or stolen.

   In addition, in 2010 LG embarked on development of its "Link Shield Service," a multi-component security scheme comprised of factory installed components, user application based components, and web-service based components. This service will give users the capability to remotely lock their devices and applications, delete certain data or information stored in the device, track the GPS location of the misplaced or stolen device, and take photos or record voices of the person in possession of the device when certain conditions indicate that the possessor may not be the rightful owner of the device (e.g., inputting wrong pass codes more than certain number of times).The Link Shield Service was launched

in Korea in February 2012, and we are currently in the process of evaluating the service and exploring the possibility of introducing this service in the United States.

2. **Do you have an evaluation process to ensure that these policies keep up with advancing technologies and changing criminal tactics?**

   As part of the development of the Link Shield Service infrastructure, we have established a sophisticated solution process designed to take into account certain technological challenges, such as service interruptions, degradation, deterioration and other service quality related issues. We also plan to establish and dedicate a specialized team in order to monitor the overall effectiveness of the security service we are providing.

3. **Law enforcement and others have suggested that the ability to disable remotely mobile devices would reduce or eliminate resale value and thus lessen the incentive for call phone theft. What are your views on this technology as a deterrent to theft?**

   Due to the very strong market that exists around the world for both mobile phones and the sensitive data stored on mobile phones, we do not believe that any technological solution can eliminate the incentives for stealing a mobile device altogether or render a lost or stolen mobile phone completely valueless. However, we are hopeful that increased utilization of existing protections by consumers, along with adoption of new technologies and services, like our Link Shield Service, will go a long way toward reducing those incentives. We are deeply committed to exploring new ways that technology can increase the security of our devices. For example, LG users who choose to subscribe and register their devices with the LG Link Shield Service will be able to lock the device remotely, or to delete certain data stored in their devices. These remote functions will be based on a unique and indelible digital imprints in each device that cannot be overcome simply by swapping out the USIM card or deleting the operating system or other software within the device.

4. **Does your company cooperate with law enforcement to retrieve lost or stolen phones? If so, how?**

   LG does not generally receive requests for assistance regarding the location of lost or stolen devices. This is due to the fact that activation and reactivation of mobile devices are not handled by the device manufacturer but by the mobile carrier, and LG does not have access to location-based or network data relating to a consumer's handset that would be helpful in the retrieval of a device.

5. **If your company has knowledge that a specific phone has been reported stolen, do you allow such a phone to be subsequently re-activated with a different phone number? If yes, please explain.**

No. Activation and re-activation of a device are controlled exclusively by mobile carriers. As discussed in Answer 4 above, LG, as a device manufacturer, is not involved in the activation, de-activation or re-activation of a device and therefore does not receive information about whether a specific device has been stolen.

6. **Australia has implemented a cell phone "blacklisting" program in which phones that have been reported stolen are placed on a list and cannot be reactivated if an individual brings them in to a local carrier. This has significantly reduced cell phone theft in Australia. Would a similar program work it the United States?**

   Because LG is not responsible for activating or re-activating mobile phones, we are not in a position to determine the feasibility of such a program.

7. **What more can be done to protect consumers? Please include any additional insights that you believe we might find helpful or relevant.**

   We think increasing the adoption of current technologies available right now, like password protection, would go a long way to reducing security risks associated with lost or stolen handsets. Better educating the consumer is an important way to increase adoption rates. We support the efforts of CTIA, the wireless trade organization of which we are a member, exploring a number of different plans for voluntary adoption by its members to address these important issues. One such plan is to implement a consumer education program regarding cell phone security, through a range of initiatives that may include a public service announcement and the use of unique websites, social media, and customer care centers. LG is also exploring ways to better educate consumers on the importance of mobile phone security by way of our user manuals and consumer website. In sum, we will continue to regard the security of the device and the user data stored in them as one of our top priorities.

LG shares your concern about the well-being of consumers, and we appreciate the opportunity to respond to your questions. Should you have any questions regarding this letter, please contact Mr. John Taylor, Vice President of Government Relations for LG Electronics USA, at 202-719-3490.

Sincerely,

Wayne Park
President and CEO
LG Electronics USA, Inc.