



April 16, 2012

The Honorable Henry A. Waxman  
Ranking Member, Committee on Energy and Commerce  
United States House of Representatives  
Washington, D.C. 20515

The Honorable Anna G. Eshoo  
Ranking Member, Subcommittee on Communications and Technology  
United States House of Representatives  
Washington, D.C. 20515

The Honorable Edward J. Markey  
Member of Congress  
United States House of Representatives  
Washington, D.C. 20515

Dear Representatives Waxman, Eshoo, and Markey:

Thank you for your letter requesting information about measures that Google takes to protect consumers in connection with the theft of smart phones.

We would like to first address Google's role in the mobile telephone ecosystem generally. Google has helped develop a mobile operating system that is used in many smart phones (a subset of mobile phones in the market). Known as Android, this open mobile operating system is utilized by various smart phone manufacturers. Today there are at least 58 original equipment manufacturers (OEMs) worldwide using Android, with over 1,000 different Android enabled-devices available on 329 wireless carrier networks. To date some 300 million Android devices have been activated around the world.

In our view, the openness of the Android platform has been key to driving innovation, adoption, and user choice. The advent of Android has created enormous opportunity for manufacturers and developers because it is a free platform on which they can build. In particular, hardware makers can differentiate their devices, creating a cycle of competition that provides users with more choice. Users are able to personalize their Android phones and download a rich variety of applications and content.

While Android is a mobile platform that OEMs and carriers choose to utilize to operate their devices over mobile networks, Google does not itself manufacture smart phones, nor do we own cellular networks or activate devices for use on cellular networks. Google is in the process of receiving government approval to purchase Motorola Mobility Inc. (MMI), an OEM. However, such approval has not been granted by all pertinent governmental authorities, so the purchase has not yet closed. Thus, at this time we cannot speak on behalf of MMI, nor can we discuss potential integration of business policies pre-close.

While Google is not in a position to discuss the practices of mobile service carriers or mobile hardware manufacturers, we wish to explain our own practices to help consumers protect their personal information if their smart phone has been lost or stolen.

Google provides mobile security tips to consumers on measures they can utilize to minimize the risks that their personal information will be accessed after their mobile device or smart phone has been lost or stolen. These mobile safety tips are available at: <http://www.google.com/goodtoknow/online-safety/mobile-security/> They include:

- Always use a passcode, password, or security pattern to lock your phone.
- If your phone goes missing, report it right away and work with your provider or police to either locate or deactivate it remotely. Change the password for your online accounts that can be accessed through your phone.

As indicated above, Google is not in the position to have policies or guidelines that operate in the same context as mobile service carriers. We do, however, continue to keep abreast of advancing technologies and changing criminal tactics and actively seek to inform consumers accordingly through our security education outreach. In addition, we welcome the April 10 announcement by the Federal Communications Commission of a cross-industry effort to deal with the issue of smart phone theft.

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

We currently have no policies or guidelines that relate to consumer mobile phone theft or loss. We do provide security tips to consumers, however, related to such theft or loss.

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

We continue to keep abreast of advancing technologies and changing criminal tactics, and actively seek to inform consumers accordingly through our security education outreach (available at: <http://www.google.com/goodtoknow/online-safety/mobile-security/>).

**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 cell phone theft. What are your views on this technology as a deterrent to theft?**

The ability to disable remotely mobile devices holds the potential to reduce theft or eliminate resale value. On the other hand, there are legitimate concerns that enabling “bricking” technology in a mobile handset could thwart efforts by a carrier to deal directly with a stolen device operating on its network, and impede the consumer’s ability to reach 911 in an emergency. The four-pronged approach announced last week at the FCC, including a “blacklisted” practice by carriers, may well represent a more measured and effective approach to the problem.

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

Google regularly cooperates with and assists law enforcement, including trainings where appropriate for the online environment. Google also cooperates with law enforcement to retrieve lost or stolen phones that are provided to its employees for business use. In particular, where a mobile phone has been lost or stolen, Google employees are required to acquire and submit a police report.

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

Because Google is not a mobile carrier, it cannot activate or reactivate mobile phones on a carrier network.

**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 into a local carrier. This has significantly reduced cell phone theft in Australia. Would a similar program work in the United States?**


As indicated above, Google welcomes the efforts of mobile carriers and OEMs to reduce smart phone theft. The initiative announced last week at the FCC includes a "blacklist" approach similar to what has been adopted successfully in Australia. There is good potential for similar success in the United States.

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

At least some of the challenges associated with smart phone theft could be addressed by more vigorous consumer awareness and education. The use of consumer education campaigns and other measures announced at the FCC last week should go a long way to reducing incidents of smart phone theft.

Google appreciates the opportunity to share its perspectives on protecting consumers in connection with the theft of smart phones and we look forward to working with Congress as it continues to explore this important issue.

Sincerely,



Susan Molinari  
*Vice President, Government Affairs and Public Policy*  
Google Inc.