Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

April 11, 2012

The Honorable Henry A. Waxman
Ranking Member, Committee on Energy and Commerce
U.S. House of Representatives
2204 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Anna G. Eshoo
Ranking Member, Subcommittee on Communications and Technology
Committee on Energy and Commerce
U.S. House of Representatives
205 Cannon Building
Washington, D.C. 20515

The Honorable Edward J. Markey
U.S. House of Representatives
2108 Rayburn House Office Building
Washington, D.C. 20515

Dear Representatives Waxman, Eshoo, and Markey:

Thank you for the opportunity to respond to your letter of March 23, 2012, in which you seek information about Microsoft's policies and features designed to protect consumers when their Windows Phones are lost or stolen. Microsoft recognizes the importance of consumer privacy and safety, and has taken these factors into account in the design of the Windows Phone operating system. We are committed to continued collaboration with device manufacturers, mobile carriers, and app developers in this regard.[1]

As described in your letter, smart phones have become a ubiquitous part of everyday life for many U.S. consumers. Smart phones literally converge historically disparate communications, personal computing, and entertainment equipment into a single device that fits in the palm of a user's hand. The convenience of these devices has unquestionably created tremendous social and economic benefits, and we are excited about the future of smart phone technologies. Microsoft looks forward to providing continued innovation and value to users of

[1] Except as otherwise specifically identified herein, this response addresses the Windows Phone 7 operating system, released in Fall 2010, and the Windows Phone 7.5 operating system, released in Fall 2011. With respect to lost or stolen phone features, there are no material differences between these releases.

Windows Phones, which in turn will create even more personal convenience, efficiency, and productivity.

We recognize, however, that the same attributes that make smart phones so popular can also create new or increased risks. Among these are risks associated with the loss or theft of phones. We believe, however, that any meaningful discussion of these risks must be divided into two distinct – albeit related – issues:

(1) the loss of personal information stored on the device (*i.e.*, the ability of consumers to protect personal information on a lost or stolen phone); and

(2) the loss of the device itself (*i.e.*, the ability of third-parties to use or resell a lost or stolen phone).

With respect to the first issue, Microsoft has designed Windows Phone to help mitigate risks regarding the loss of consumers' personal information. Windows Phone includes several features that enhance users' control over personal information on a lost or stolen phone. As described in more detail in response to your questions below, users can employ a "lock screen" and password feature on the phone itself. Moreover, users can also remotely find, lock, and/or erase their phone from any computer web browser. Windows Phone users can also store copies of much of their phone data, such as photos and apps, "in the cloud" in order to facilitate recovery of the information if their phone is lost or stolen, or if they choose to "erase" their phone.

With respect to the second issue, however, we believe any practical mitigations likely fall outside the sphere of operating system design. Although blacklisting programs, such as the one you described in your letter, have been adopted to deter theft, the implementation of such programs would likely fall primarily to mobile carriers. Accordingly, we defer to the carriers in addressing the potential implications of such programs.

With this information as background, Microsoft responds below to your specific questions.

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

As summarized above, the Windows Phone operating systems contain several features designed to help consumers retain control over their personal information if their phone is lost or stolen:

A. Lock Screen (On-Device)

Windows Phones provide consumers the ability to manually lock their phone at any time, or to have it automatically lock after a user-defined period of inactivity. To unlock the phone, a

user must enter a user-defined password (PIN). Details on the Lock Screen feature can be found at http://www.microsoft.com/windowsphone/en-US/howto/wp7/basics/copy-and-paste.aspx.

When a phone is locked, users may still perform a few convenience functions (*e.g.*, make an emergency call, see incoming caller identification data, and take a photo using the camera). As a practical matter, however, when the phone is locked the consumer's personal information is unavailable to all but the most sophisticated third party that obtains possession of the phone.[2] Nevertheless, the lock feature may not prevent a complete reset of the phone to factory settings. Thus, while protecting the consumer's personal information, the lock may not prevent a third person from obtaining value from the resale or use of the phone itself.

Most smart phone users are familiar with on-device passwords – based on interactions with personal computers and the web. Although Microsoft recommends that consumers use the lock feature and employ device passwords,[3] except in certain instances associated with corporate phones, we do not mandate such use.[4] We believe this should remain a matter of consumer choice.

B. Find, Ring, Lock, & Erase (Remote - via web)

Windows Phones also provide a consumer the ability to remotely locate, ring, lock, and/or erase his/her phone data from any computer with web access – even if they no longer have possession of their phone. These features are made available by Microsoft at no additional cost to any Windows Phone user who has associated a Windows Live ID with their phone.[5] (Windows Live ID is also the mechanism used to authenticate users in the Windows Phone Marketplace – which provides apps, ringtones, etc.) Details on these features can be found at http://www.microsoft.com/windowsphone/en-US/howto/wp7/basics/find-a-lost-phone.aspx.

---

[2] As with all computers, a level of technical expertise may allow a person to recover some data from a Windows Phone despite password protection.

[3] *See* Windows Phone Privacy Statement ("Security of Your Information") at http://www.microsoft.com/windowsphone/en-us/privacy.aspx and "Tips to Keep My Phone Secure" at http://www.microsoft.com/windowsphone/en-US/howto/wp7/basics/tips-to-help-keep-my-phone-secure.aspx.

[4] If a user seeks access to corporate-administered e-mail accounts on their device, the corporate administrator may require the user to password protect their device. In that case, the Windows Phone operating system can be configured to prompt the user to set a mandatory password (PIN) and configure the lock feature. The lock feature can be configured in a manner that the phone's data will be erased automatically after a pre-determined number of failed attempts to enter the proper PIN. If no corporate-administered password is enabled for a device, the phone will deter access to the phone by creating increasingly long delays for a user to enter a proper PIN after five unsuccessful attempts. This adds a measure of protection against unauthorized access to the phone in cases where no corporate-administered access policy has been enabled, and in any case, users may choose to manually lock the phone at any time.

[5] Depending on the user's mobile carrier plan, the carrier could charge the user for data usage and SMS activity associated with these features.

(1) Find My Phone

A Windows Phone user can remotely locate his/her phone's approximate location on a map, by signing into "My Phone" at https://www.windowsphone.com/en-US/my. If the user's phone is on, has battery power, and is within carrier range, this feature uses text messaging protocol to locate the phone and display its location on a map.[6] Users can also choose to save their location every few hours so that they can still see their phone's last-known location on a map if their phone is out of carrier range or the battery dies.[7] When using this feature, only the most recent location of the phone is stored and retained by Microsoft. If users believe their phone is within range of their hearing, they can also "ring" their phone from the web. When using this feature, if the phone is on and has battery power, a loud and distinctive ring tone will be audible even if the volume is turned off or the phone has been set to vibrate mode.

(2) Lock My Phone

A Windows Phone user can also remotely lock his/her phone by signing into "My Phone" at https://www.windowsphone.com/en-US/my. If the user's phone is on, has battery power, and is within carrier range, this feature will lock the phone even if the user has not previously set a lock screen password. In that case, the user will be prompted to enter a password via the web to use when they get their phone back. After locking the phone, it will behave in the same manner as if it had been manually locked using the lock screen feature previously described. Users can also optionally display a message on the phone's screen – typically an alternative phone number or an e-mail address that can be used to contact the owner if someone finds the phone.

(3) Erase My Phone

Lastly, a Windows Phone user can remotely erase his/her phone by signing into "My Phone" at https://www.windowsphone.com/en-US/my. If the user's phone is on, has battery power, and is within carrier range, this feature will remove all user data from the device – such as message content, photos, music, etc. This feature effectively returns the phone to factory settings.[8]

Notably, most of these features are intended to assist users primarily in the case of a misplaced or lost phone, or in the immediate aftermath of a phone theft. The features cannot work if the phone is turned off or has no battery power, or if its battery has been removed. Similarly, these features will not work if the phone's SIM card has been removed or replaced, or the phone has been transferred to a different carrier account.

---

[6] Users can also choose to configure their phone to use "push notifications" instead of SMS for this purpose. The use of push notifications may use more battery and must be set by the user in advance, while in possession of the device.

[7] Once again, this feature must be enabled by the user in advance, while in possession of their device.

[8] Although beyond the scope of this response, Microsoft also offers users the ability to configure their devices to store copies of certain information, such as contacts, photos, and information about downloaded apps, on Microsoft servers ("in the cloud"), which may prove helpful to users who find it necessary to erase their lost or stolen phone.

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

Microsoft employs an extensive, systematic evaluation process with respect to the design and testing of all Windows Phone operating system features. As previously described, we have deployed Windows Phone features designed to help ensure the protection of consumers' personal information – including on lost or stolen phones. We will continue to place these issues at the forefront of our design efforts, and we look forward to offering expanded features in upcoming versions of the Windows Phone operating system.

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?***

Microsoft believes the capabilities outlined in your letter are useful to protecting personal data contained on lost or stolen devices. For that reason, we provide Windows Phone users the ability to remotely find, ring, lock, and erase their phones, as outlined above. Such features may deter cell phone theft if the thief's primary motive is gaining access to user's personal information. Such features will not, however, deter cell phone theft if the thief's primary motive is to simply obtain the phone for its potential resale value.

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

This issue will typically be more applicable to the mobile carriers. Upon receipt of valid legal process, however, Microsoft will disclose to law enforcement officials responsive records in its possession or under its control, which may aid law enforcement in retrieving lost or stolen phones. In many instances, the law enforcement requests do not disclose the reason for or nature of the underlying investigation. Accordingly, even if contacted by law enforcement, Microsoft may not be aware that the request is related to thefts of Windows Phones.

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.***

Microsoft does not play a direct role in the activation of phones or the assignment of phone numbers.

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 in the United States?***

As summarized above, Microsoft believes there are a number of issues that would need to be addressed before such a program could be deployed in the United States.

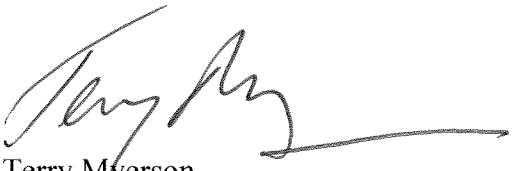
7. ***What more can be done to protect consumers? Please include any additional insights that you believe we might find helpful or relevant.***

Consumer privacy and safety have been, and will remain, an important aspect of Microsoft's design of the Windows Phone operating system. We strive to provide consumers with tools to protect their personal information – including when their phone is lost or stolen – in a way they can easily understand and use. We believe such features are generally effective. However, there is always room for improving consumer education and awareness (*e.g.*, simply increasing certain consumers' willingness to use features that automatically lock their phones after a period of non-activity could substantially improve the privacy and safety of their information in many instances). Microsoft is certainly willing to explore such opportunities.

* * *

Again, Microsoft appreciates the opportunity to provide you with this information. Please direct any further questions regarding this matter to the undersigned.

Respectfully submitted,



Terry Myerson
Corporate Vice President
Windows Phone Division