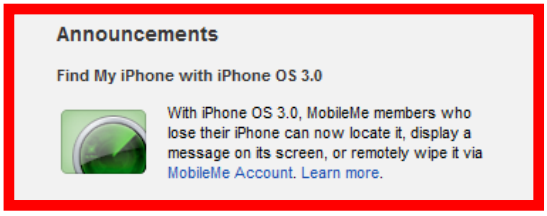
6/18/2009

# AWARENESS BRIEF

## FIND MY IPHONE

# Computer Crime and Intellectual Property Section Cybercrime Lab
# Awareness Report: Find my iPhone Feature

Researched June 17, 2009
iPhone 3.0 Operating System, Find my iPhone Feature




## Summary:

On June 17th, 2009, Apple launched version 3.0 update to the iPhone and iTouch operating system with several new features. Two new feature of possible concern to law enforcement include:

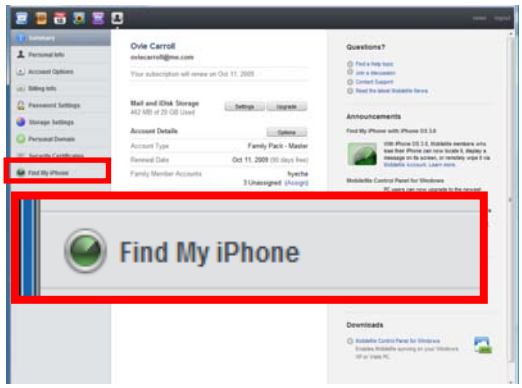


Figure 1

**Feature 1**. The ability for users of iPhones to log onto their mobile me account from any web browser and see the geographic location of their iPhone.

This feature is free and can be done as often as they desire. To use this feature, from the mobile me web interface, users click on the "Account" icon, then select the "Find my iPhone" icon at the bottom of the left sidebar (see figure 1). The location of the iPhone is immediately queried and if the phone is connected to an Edge or 3G network the location is displayed on the map. (see figure 2)

Figure 2

**Feature 2**. Of greatest concern to law enforcement is the ability for the user to remotely wipe all data from the phone. Using this feature will delete all data from the iPhone, including emails, account information, applications installed, music downloaded, etc. Once the wipe feature has been activated all data is wiped and the phone is restored to the default factory setting. Once the phone is back to the default factory settings, all other "find my iPhone" features will no longer work (e.g. you will no longer be able to query the location of the phone, send a message or cause the phone to emit a tone). Because all information from the iPhone is backed up to the iTunes application on users computer system, a user can easily restore their iPhone to the state of it's last backup by synchronizing it again to their iTunes application.

The ease of restoring the iPhone to it's last backup condition may encourage users who's phones have been temporarily seized by law enforcement to wipe all data to

prevent law enforcement from gaining access to it.

Law enforcement seizing iPhones as potential evidence are recommended to protect the phone from wireless signals as soon as possible through the use of a faraday bags or some other nickel, copper and silver plated storage container (see figure 3). The device must be protected from any wireless connection/radio signal even throughout the forensic imaging process.


Figure 3

Another feature available in the version 3.0 operating system, although not as significant to law enforcement is the ability for users to cause the phone to both display a message and/or emit a two minute tone so users can locate the phone by following the sound. The message and tone will display if the device is powered on and connected to an Edge, 3G or WiFi network, even if the phone is set to silent or vibrate only mode. If the phone is not powered on or not connected to a network, the message and tone will display the next time the device is online.

The owner of the account will also receive an email message to their mobile me account verifying the message was received/displayed by the iPhone (see figure 4).

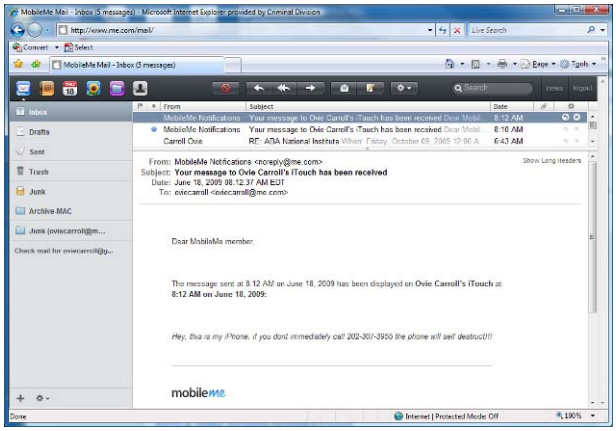



Figure 4

Law enforcement who personally use or have confidential informants using iPhones with this feature should give consideration to disabling this feature until additional analysis can be conducted to ensure criminal elements can not activate this feature without the user being notified.

While the implications may be obvious, It is something we all need to be aware of when consulting or assisting on investigations and worth recapping.

## POSSIBLE IMPACT ON LAW ENFORCEMENT

1. It may be possible to locate the user of an iPhone using this “find my iPhone” feature. (with appropriate legal authority)

2. If compromised, this feature may allow criminals to locate the user of an iPhone. Law enforcement who personally use or have confidential informants using iPhones with this feature should give consideration to disabling this feature until additional analysis can be conducted to ensure

criminal elements can not activate this feature without the user being notified.

3. Law enforcement and the courts should be made aware of the potentially exigent circumstances that have been created by this remote wiping feature that requires rapid actions to be taken to safeguarding and or image iPhones encountered during criminal investigations to prevent the loss of valuable evidence or investigative information.

4. Forensic analysts that receive iPhones in a faraday bag or other protective storage device, must ensure that the phone is kept in a protected environment and not permitted to ever receive radio signal subsequent to the device's seizure, throughout the imaging process to prevent the device from connecting to any network and receiving and commencing the wipe command.

**Recommendations:**

1. Conduct conference call with Apple iPhone technical representatives to gain a better understanding on how this feature can be used and what privacy safeguards have been implemented to prevent unintended use.

2. Conduct conference call with Apple iPhone technical representatives to determine if this feature can be used to aid in the identification of kidnapped or missing persons investigations without jeopardizing their safety.

3. Ensure all law enforcement and incident responders are aware of the remote wiping capabilities of the iPhone and equip them with faraday bags.

4. Ensure law enforcement is aware that a back up of all data on the iPhone may be contained on a computer system. Law enforcement should consider seeking authority to seize any computers possibly used to backup/synchronize an iPhone.