“The FBI vs Apple: Look to Mobile Device Management (MDM) software to Access Enterprise Owned Smartphones Used by Criminals and Terrorists”*

Syed Rizwan Farook was issued his iPhone by San Bernardino County. He signed over rights to the data on the device. While Mobile Device Management (MDM) software had not yet been installed on Farook’s iPhone, MDM software will help resolve legal issues for corporate issued devices in which MDM software is installed.

Figure 1. Terrorist Syed Rizwan Farook and what may be a photo of his iPhone 5c that was owned by San Bernardino County.

Wednesday, March 2, 2016

Written By:

J. Gerry Purdy, Ph.D.
Research Director, MobileSolve Group, Inc.
Principal Analyst, AOTMP
gerry.purdy@mobilesolve.com
404-855-9494

The issue of privacy and the law – particularly with respect to terrorism and the FBI – is challenging. A number of people have asked me where I sit regarding the current high profile case between the FBI and Apple over the iPhone that was recovered from Syed Rizwan Farook after his terrorist attack against employees of San Bernardino County where he worked.

While I do believe in privacy and individuals keeping their own information confidential, I also believe in the rule of law and, in particular, special provisions in any democracy to deal with mobile devices obtained by law enforcement from terrorists or others that break the law. Thus, I believe in protecting the information in devices owned by individuals but point out that information on enterprise owned smartphones is owned by the enterprise.

In the case of Mr. Farook's iPhone, it was owned by San Bernardino County. The County was in the process of implementing Mobile Device Management (MDM) from MobileIron that would enable the County to access any/all of the information on the phone. It's too bad that the full MDM software wasn't yet installed on Mr. Farook's iPhone. If it had been, then the County could have accessed the information and provided it to the FBI.

The County had begun the process. It had already implemented the MobileIron email component that enables County employees to access their County email using their iPhone. The next step was to add full MDM software so the device could be remotely managed, wiped clean if necessary or accessed as required by any law enforcement or government agency with proper court order.

Clearly, the FBI should be also be dealing with San Bernardino County. It would seem to me that since the County owned the device, they could join with the FBI to request the bypass to

the automatic trigger that would wipe the device clean after 10 unsuccessful password entry attempts. This issue must be resolved by the courts.

The MDM software from MobileIron is similar to what other MDM providers offer such as AirWatch by VMware, Citrix Systems and IBM.

Thus, in cases where the device in question is owned and issued by an enterprise (vs. owned by the individual and not operating with the user's enterprise network), it will be much easier to resolve requests by law enforcement and government agencies.

Going forward, we need to have some way to deal with the issues of mobile devices that are used by people for illegal activities. I leave it the courts and law enforcement (including the FBI) to address the issue.

I have put the different kinds of mobile device ownerships and access methods together in Figure 2.

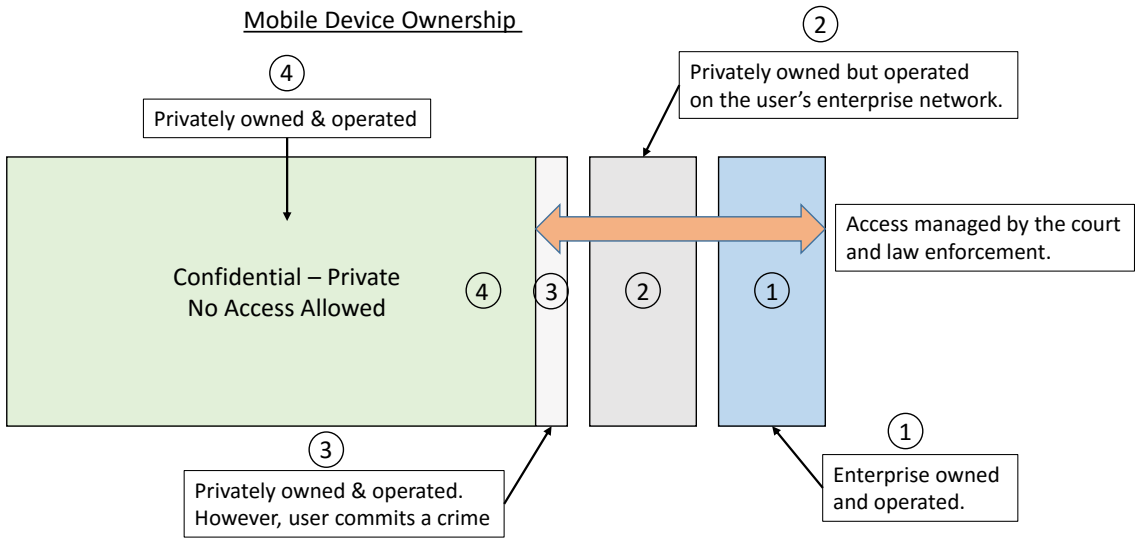

Figure 2. Mobile device ownership and oversight with provisions for appropriate access.

There are four different scenarios:

1. Enterprise owned and operated – In this scenario, the mobile device is owned and operated by the enterprise. The organization has MDM software installed that enables the enterprise to see the information that's on the device at any time. If the enterprise doesn't have MDM software, then they hopefully will have the information stored in a backup.
2. User owned but enterprise operated – The user owns the device but it operates on the enterprise network. At that point, the user has agreed that all of the enterprise

information on the device is owned by the organization. The information that is owned by the user (e.g. their photos and music) can remain private and confidential by the owner. This is typically enabled through the use of digital locker in which the enterprise information is placed and held separate from the user's personal data.

3. User owned but crime committed – The user owns the device but then he or she commits a major (felonious or terrorist) crime. The courts and law enforcement decide what to do. If a 'back door' is ruled to be required, then perhaps OS vendors like Apple (iOS) and Google (Android) will be required to enable that kind of access.
4. User owned with no crime committed – In this scenario, the user owns the device and he or she has not committed a crime. In this scenario, the information is kept confidential.

Now, when there is a court order with adequate law enforcement (including the FBI) justification, each of the four situations is handled as follows: (See Figure 3.)

1. Enterprise owned and operated – The enterprise uses their MDM software to download the user's data and provides it to the law enforcement organization, including the FBI. This was the ownership and operation class that the terrorist was operating under in San Bernardino County. However, the County had not yet installed the components of the MobileIron MDM software to manage the contents of the device.
2. User owned but enterprise operated – Once the user agrees to have his or her smartphone or tablet run on the enterprise network, then the enterprise has rights to the enterprise information. The enterprise either uses their MDM software to access and provide the information to the law enforcement organization or if MDM software isn't installed, then they would have to provide the information from a backup that most organizations do. If the law enforcement organization needs access to the personal information, then they get the court order to do that. (I'll let the courts, vendors like Apple and law enforcement organizations like the FBI work on resolution of how/when to provide access to a user's information).
3. User owned but crime committed – Hopefully, this scenario, the user's data is protected, but since we operate under the rule of law, if a (felonious or terrorist) crime has been committed and there's a court order, then the courts and law enforcement will have to determine if the information must be accessed. The OS vendors then need to work out a way to enable that to happen.
4. User owned with no crime committed – When the user owns the device and no crime has been committed, then there should be no way in which anyone other than the user can access the information in the user's mobile device.

Authorization for Information Access on Mobile Devices

Mobile Device Ownership & Operation	Who Provides the Information
(1) Enterprise owned & operated	Enterprise provides information from MDM
(2) User owned & enterprise operated	Enterprise provides their information from MDM. Courts & law enforcement decide about personal data
(3) User owned & crime committed	Law enforcement & the courts decide.
(4) User owned	Access not allowed

Figure 3. Management of Authorization for Information on Mobile Devices

Relative to the current case of the terrorist having been employed by San Bernardino County, the FBI should be working with San Bernardino County and together deal with Apple. Unfortunately, the County had not yet installed the necessary MDM device management software on Farook's iPhone.

I leave it to congress, the courts and law enforcement agencies to determine to what extent personally owned but locked smartphones should be able to be unlocked by anyone other than the owner.

* Republished with permission by AOTMP.

If you would like to receive this newsletter directly, send your contact information to subscribe@mobilesolve.com or go to www.MobileSolve.com.

Disclosure Statement: From time to time, I may have a direct or indirect equity position in a company that is mentioned in this column. If that situation happens, then I'll disclose it at that time.