Smartphones for Lawyers: Selecting, Managing and Securing Them

by Sharon D. Nelson, Esq. and John W. Simek

Unless you've been trying to emulate a hobbit and have been living under a rock these last few months, we're fairly certain that you have heard about the consumerization of smartphones across the country. Perhaps you've heard the term, but don't really know what it means. Essentially, it is the insistence by employees that they be allowed to bring their own (consumer) smartphones into the workplace environment and access the corporate data (e.g. e-mail, client files, billing system, etc.). The Bring Your Own Device (BYOD) or Bring Your Own Technology (BYOT) movement is putting severe pressure on all forms of business, including law firms. Before we get to the issue of dealing with the BYOD and BYOT movement, let's speak to the selection of smartphones.

The first decision point is whether you will allow employees to use their own devices or if you are going to distribute firm owned devices. Frankly, we are not fans of BYOD or BYOT and prefer that the firm provide the mobile devices directly to the employees. It makes it much easier to set the policies and controls when the firm owns the asset. There is little argument about what the firm wants to do with devices that they purchased, but you may be in for heated battles if you try to control an employee-owned device.

If you allow BYOD or BYOT, then your decision process is done as far as equipment goes. The employee has already made up their mind what device to purchase. If the firm will select the mobile device (smartphone, tablet, netbook, etc.) then the first place to start is with a wireless carrier. Define where you intend to use the devices and pick the carrier that has the most reliable service for those areas. Once you've picked the carrier, you can then move to the devices that they have available. Perhaps you're absolutely sold on touch screen technology. The carrier will have certain models that they support, thereby narrowing the field. You may be looking for a specific feature, such as memory (storage) expansion. That rules out the iPhone since it is a fixed memory device. No matter what you decide, choosing the carrier first will necessarily restrict the devices that are available for your selection.

When it comes to smartphones, security is a very important element, especially for attorneys since they have an obligation to protect their client's information. This is where things get a little muddy. Some say that the BlackBerry is the most secure smartphone because of the inherent encryption on the phone and in the communication. Partially true, but you can also encrypt an Android phone. In fact the DoD has recently approved a specific version of the Android OS for use with non-classified information. This is hardly surprising with the explosion of smartphones running the Android OS. Also, don't forget to encrypt the contents of the expansion card if available. You may need some third-party software to get certain functions so don't just look at the base phone.

Besides the features, there are some basic security measures that you should take with any smartphone no matter what OS you use.

- Encrypt the data on the phone and expansion card
- Maintain physical control of the phone – in other words don't lose it!
- Follow any security recommendations from the carrier and phone manufacturer
- Program a lock code (e.g. PIN, passphrase or password)
- Set the phone to automatically lock after a period of inactivity
- Limit the amount of confidential data stored on the phone
- Turn off any interfaces that are not used (e.g. Bluetooth, WiFi)
- Have some method to backup your data
- Only use secure (e.g. https) connection for web browsing
- Configure the ability to remotely wipe the phone if it is lost (may require third-party application)
- Install security applications such as antivirus, malware protection and encryption (may require third-party application)
- Do not "root" or "jailbreak" the phone
- Only install applications from trusted sources (iTunes is not immune to malware apps and be particularly cautious in the Android store)
- Avoid using unknown WiFi clouds

Securing the data on your smartphone should be your primary consideration. Yes, the iPhone is encrypted, but it is a fairly weak encryption scheme. The latest version of the Android OS (Ice Cream Sandwich) now includes encryption. The data on a BlackBerry is encrypted by default. It really doesn't matter which OS you use since some encryption is better than none. For gosh sakes, don't use a phone that is not encrypted and doesn't have any third-party applications to make it secure. In addition to the encryption, install a security application to the phone. This will help protect against such things as malware and those bad URLs. Companies such as Symantec, Trend Micro, Sophos, etc. have mobile security products for different operating systems. Some manufacturers claim to have security products for the iPhone. They perform such functions as malware scans (after you've already downloaded the malware), device location, remote wipe, identifying unsecure WiFi, data backup, etc. Unfortunately, there really aren't any adequate security products for the iPhone. Apple doesn't allow any third-party application access to the lower levels of the OS, where effective security applications must reside.

So let's get back to the BYOT and BYOD concept. How do you manage the devices that you don't own whose owners want to access data on your network? For that matter, how do you manage devices that you do own? The simple solution is to use a Mobile Device Manager (MDM). If you have ever worked with a BlackBerry Enterprise Server (BES), then you've dealt with a MDM. The MDM sits between your infrastructure and the mobile device. It controls the mobile device (including things like the iPad) and provides additional security features. The MDM function can be installed within your network or can be provided as a hosted solution. The hosted option may be a good choice for a lot of smaller firms since they won't have to potentially invest in hardware or licensing costs. Be sure to check with your cellular carrier to see if they offer hosted MDM solutions, which may be bundled with your cellular service.

The MDM provides a lot of control for your mobile devices. A base level function is to identify what devices are connected to your network. You can't control it if you don't know it exists. Since the MDM

operates as a “gateway” to the data, you have vision into each device trying to access the information. The MDM also enforces policies to the device. This could be such things as the requirement to have a password, PIN, etc. and the complexity (e.g. 12 or more characters) of the lock code. The policy can also enforce encryption of the device and any inserted expansion cards. You can also disable certain features of the device via the MDM. As an example, perhaps you don’t want any Bluetooth devices to be used. Bluetooth can be disabled for all phones or perhaps just one. You have the ability to locate and remotely wipe the device. Some MDMs will create a “sandbox” area on the smartphone and the remote wipe will only impact that area. This feature may be useful if you are allowing BYOD. Wiping the “sandbox” would leave the entire user’s personal information intact while clearing out the firm data. Another feature is to allow only the installation of approved applications and prevent all others. Be prepared to get some push back if you implement application control, especially if it’s the employee’s smartphone.

Two of the highly regarded MDM solutions are provided by Good Technology (www.good.com) and Mobil Iron (www.mobileiron.com). They can manage smartphones running a variety of operating systems all at the same time. This means you could have iPhone, Android, Windows Mobile and Symbian smartphones throughout your firm and still maintain control. Obviously, it would be better to standardize on one phone OS, but with many MDMs you have options.

Research in Motion’s MDM (RIM) (www.rim.com) has been long considered to be the gold standard in mobile device management and security. However, its market share has been rapidly declining and some analysts have questioned its long term survival. In May of 2011, RIM purchased ubitexx, a German provider of MDM software. After the acquisition, RIM announced that it would use the ubitexx technology to support management of iPhones and Android phones through BlackBerry Enterprise Server. The product is named BlackBerry Mobile Fusion and the scheduled release is March 2012. It will support BlackBerry, Android and iOS devices; however, it will only support the native abilities of the device for Android and iOS devices. We’ll have to see if their new MDM will help keep RIM afloat, but we have our doubts.

No matter which platform or smartphone you decide to support. A key consideration is to maintain the security of the information that is stored on those nifty little devices. Remember, besides playing games, smartphones do hold confidential client information.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com