Lawyer's Duty of Confidentiality and Securing Your Smartphone and Handheld Device

by Wendy F. Inge

What's not to love about a smartphone? It's a great tool for keeping up while on the go. And smartphones aren't just phones; they're computers. The use of smart phones and other mobile devices such as iPads is pervasive, and lawyers too have embraced them.

But as with all technology used by lawyers, we have certain ethical duties that apply. State bars have consistently held that the use of technology, such as e-mail, cloud computing and portable devices requires consideration of the rules of professional conduct addressing competency and confidentiality. Specifically, lawyers using this technology should be competent in understanding the technology (*Rule 1.1 Competence*) and how its use might impact the client either positively or negatively. Also, the lawyer needs to act diligently to protect client confidences and ensure that client information remains secure (*Rule 1.6 Confidentiality of Information*).

Inherent Risks

As we all know, the risks inherent in using any device that stores or accesses our data are that it will be hacked, corrupted, misused, or stolen. Specific to smartphones, hacking and corruption can occur through the downloading of applications that are corrupted or contain malware. Theft of information can occur if the device is lost or stolen. In order to protect the sensitive information and the client, and to fulfill your ethical duties, you must secure your mobile devices.

Who Owns the Device?

One of the first things to consider when giving employees access to client and corporate data remotely is who is going to own the device. It may be preferable from a security and policy standpoint for the firm to own the mobile devices used by employees. It makes it easier to set policies and controls when the firm owns the asset. This also allows the firm to select the wireless carrier and the device that will be used by the employees.

If you don't own the devices being used by employees to access data on your network you may want to consider using a Mobile Device Manager (MDM). An MDM sits between your infrastructure and the mobile device. It can be installed on your network or provided by a host, such as your wireless carrier. It allows you to identify what devices should be allowed to connect to the network and can regulate security policies that are to be applied to the devices. To read more about MDMs, see *Smartphones for Lawyers: Selecting, Managing and Securing Them* by Sharon Nelson and John Simek of Sensei Enterprises.

Securing Your Mobile Devices

Your firm should make it a policy that lawyers and staff using mobile devices that have access to client information follow these security procedures.

Encrypt Data: Encrypt the data on the phone and the expansion card if applicable. BlackBerry, Android varieties, and iPhones have varying levels of encryption available. (Many argue the Blackberry is the most secure because of the inherent encryption on the phone and during the communication.) You may need additional third-party software to get certain functions to upgrade the base phone if necessary. Just note however that for iPhones third-party software for encryption is not available.

Manufacturer's Security Recommendations: Follow security recommendations from the wireless carrier and phone manufacturer**.**

Password Protection: All smartphones, tablets, laptops, and mobile devices must have password protection. Your firm should have a password policy for all mobile devices (desktops too) requiring use of a strong password prior to use of the device. Use power on passwords and enable auto-lock features (phone automatically locks after a period of time) to protect all devices that carry data about a client or their matter. If able, use a strong password that is a combination of uppercase and lowercase letters, numbers, and symbols, and is a minimum of eight characters long. For more on smart passwords see *Don't Trifle with Password Safety* by Vivian Manning. Also, some apps will allow you to set up an additional pass code. If you are using an app that will contain sensitive data, create an additional pass code. Finally, some smart phones, like the iPhone, can be set to erase all data after ten failed attempts to

login; this feature provides additional security if the device is lost or stolen.

Physically Protect the Device: Keep your device with you and under your control at all times. (Don't lose or misplace it, or lend it to others.)

VPN Connection Only: If using the device to connect to the office network, only ever do so by way of a secure VPN connection. Text messages, email, and documents should never be sent in an unencrypted format, which means don't do any work using a Wi-Fi signal.

Limit Bluetooth: Only enable Bluetooth functionality when you need to use it. For all other times, turn it off.

Backup Your Data: Devices do get lost, are stolen, or sometimes simply get destroyed. Accidents do happen, so make sure any critical data is backed up.

Remote Data Wipe: Install and use a remote data wipe application on all mobile devices. This may require a third-party application. If your phone or device were lost or stolen you need to be able to wipe the data clean so that the thief or others would not be able to hack into it (because of course it has a strong password.) The Android market has hundreds of different apps that will provide this service, some free and some for a fee, but be careful to install only a reputable product (AndroidForums.com). You should pick one that is highly rated and that comes from a reliable source such as the Android market place (Google) or the iPhone app store. Droid users might want to consider "Lookout Mobile Security" and for iPhones use the iCloud functionality under settings. Be advised that applications do change security settings on your phone, and you need to be comfortable with the changes the application will make. Pick one and use it. Some, such as "Where's My Droid" and iCloud, will give you a GPS fix on the location of your device.

Install Security Application (prevents viruses, malware and bad URLs): While technology experts debate whether and to what degree smartphones are susceptible to viruses, trojans and malware have already been used to attack hand held devices. If you have sensitive information on your device, it is "better safe than sorry." Corruption of data can be a nightmare and expensive to fix. You want an application that will scan for bad actors and eliminate threats. Thus, you should require all mobile devices to be protected with anti-virus software. There are hundreds of apps for this, some free and some for a small fee, but be careful to install only a reputable product (AndroidForums.com). You should pick one that is highly rated and that comes from a reliable source such as the Android market place (Google) or the iPhone app store. For droid users consider "AGV Antivirus Pro." For iPhone users check out "Virus Barrier." Some products will provide both antivirus protection and remote wiping ability.

Corruption of data can be a nightmare and expensive to fix.

Applications: Do your research and only install applications from trusted sources. There have been problems with malware apps when downloading from iTunes and caution is even required in the Android store.

Equipment Upgrades: When the time comes to upgrade user phones, make certain that all data on the old phones is wiped prior to recycling. One way this can be done is by resetting the device to factory settings. Prior to taking this step, however, make certain that any data you want saved has been copied to another device or computer prior to restoring to factory settings. Be aware that factory resets do not erase data on any microSD cards. That data must be taken care of separately.

Finally, a disclaimer. This risk management information is provided by ALPS as general information only. It is not intended to be used or relied on as legal advice. Also, as technology changes quickly, this information may become out-dated. ALPS does not endorse any products. Readers should always engage in their own research and evaluation of products and services.

Wendy Inge is the Virginia risk manager for Liability ALPS, the Virginia State Bar-endorsed legal liability insurer. She is available to answer risk management questions at no charge for all members of the VSB. She can be reached at (800) 367-2577.