Securely Deleting Data from Mobile Devices

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

Why do we care about deleting data from mobile devices? Usually, we are trying to get back data that we inadvertently deleted. It could be that we "fat fingered" an e-mail or text message or blew away a photo that we really wanted to use as a background image. But what about when we are upgrading our smartphones, iPads or other mobile devices? Do you really know what confidential or personal information resides within the memory of your prized possession? As lawyers, we have an ethical obligation to protect the information of our clients. This means that we better be darn sure the data doesn't stay on our smartphone when we sell it, give it to our kids or donate it to a worthy cause.

Many lawyers don't believe there is any confidential information of their mobile device, especially if they never specifically took steps to save any data. The unfortunate truth is that smartphones, iPads, etc. automatically save data even if you don't want them to. As an example, every time you hit the "home" key on an iPhone, a screenshot is saved to the phone. What if you had an attachment open? A picture of that attachment now resides on the phone even though you didn't explicitly save the attachment. Data is automatically saved on other platforms too, so it is best to assume that your mobile device does contain confidential information that must be removed. The ability to securely delete data varies by operating system and platforms. Some are built-in and some require third party products.

Let's start with one of the easier platforms to deal with – BlackBerry. BlackBerry devices have a built-in feature to securely delete data. Navigate to Options. Select 'Security Options' and then 'Security Wipe'. You will need to confirm your wipe selections and intent by typing the word "blackberry" at the bottom of the screen. Once confirmed, the device will clear the selected data. The procedure is slightly different for older versions of the OS. Wiping the PlayBook is similar as well and accessed through the Settings icon. As an alternative, you can remotely wipe the BlackBerry if you are connected to a BES (BlackBerry Enterprise Server). The administrator issues the remote wipe command from the BES console and no user action is required.

There are a couple of different ways to clear the data from the iPhone, iPod Touch and iPad. The more difficult method is to use iTunes to restore the device back to factory defaults. First launch iTunes and connect the device. Select the device and click on 'Restore'. You will be prompted to back up the device. It is up to you whether to back up or not. Following your selection, there will be a prompt to restore the device to factory defaults. Click the Restore

button and the process will begin. You will receive a confirmation message once the device is restored to the original factory settings. Like the BlackBerry, remotely wiping is an option.

Apple has changed the method for remote wiping from the original Find My iPhone application. You are now required to sign up and configure iCloud in order to use the Find My iPhone service. Make sure you read the Terms and Conditions when agreeing to use the iCloud so that you understand what Apple can do with your data. We've already written an entire article about iCloud Terms and Conditions so we won't rehash it here. Once you have set up and enabled iCloud, you need to configure the Find My iPhone app on the device. Essentially, you need to turn it on, but you're not done yet. Download and install the free Find My iPhone app. The app allows you to locate the device if it is lost and remotely wipe the data. You won't be able to remotely wipe the data if you haven't configured and installed the appropriate software prior to initiating the wipe request. Understand that once you initiate a remote wipe, the device will be reset to factory defaults. This means you won't be able to find out where the device is located. You may elect to do a remote wipe instead of using iTunes, especially if you are in possession of the device.

Android devices are trickier to deal with, primarily because there are so many variants of operating systems and manufacturer capabilities. We certainly don't have the time or column inches available to run through all the variations. The simplest way to clear the data from an Android device is to reset it to factory defaults. This is done by going to Menu -> Settings -> Privacy -> Factory data reset. If you care about the information on the phone, make sure you back it up prior to resetting the phone. Is the data really gone when you factory reset? It's hard to tell without testing each and every phone and operating system combination. The short answer is probably not, but it's good enough. Forensic software and techniques may be able to recover data after a factory reset, but "Joe Six Pack" isn't going to be able to retrieve it.

While we're on the subject of factory resets, almost all other mobile devices are cleared in this way. Here is where Google is your friend. Do a search for how to factory reset your particular mobile device and we're sure you'll find the procedure. We had an attorney contact us and he wanted to know how to get rid of some nasty program that had infected his feature (non-smartphone) phone. His phone was acting strangely after clicking on a link in a text message that appeared to come from his son. We told him to Google the manufacture, model and term "factory reset" to get the instructions. He was very grateful to have his phone back to normal operation. [Note to self: Don't click on things you shouldn't!]

Finally, don't forget to wipe the data from any memory expansion cards that may be in the phone. The iPhone users don't have to worry about this since you can't expand the memory, but all others may have a 2GB, 4 GB or larger SD or micro SD card for memory expansion. The card may contain attachments, pictures, etc. that should be wiped prior to disposal. There are

several alternatives for dealing with these memory cards. The easiest is to just remove them and don't give the cards away. More often you will want to give the cards away and need to wipe the data. You can remove the cards from the phone and put them in a computer that can read the contents. Sometimes you can just connect the phone (with the card installed) to a computer and see the memory card contents. Once you can access the card, use software to wipe the data. A product like BCWipe will do the trick, but there are many others available.

Remember – the best tip in this article is to Google the method to remove the data from your mobile device. The advice we've given is current as we write, but as we know too well, things change in one heck of a hurry in the legal tech world.

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