Legal Ethics: Check Your iOS 8 Privacy Settings

by Christopher B. Hopkins

In September 2014, Apple released its new iOS 8 mobile operating system which changed functions and privacy standards. If you update an existing device or buy a new one, there are ethical implications to how you configure your iPhone or iPad. Rule 4-1.1 requires competent representation which includes knowing the benefits and risks of new technology. Rule 4.1-4 demands that client communications be prompt and reasonably thorough. If you text (SMS) with a client, you are likely aware of the challenges since SMS messages are short, difficult to save, and they appear on your lock screen without warning. Ethics Opinion 10-2 and Rule 4-1.6 insist upon confidentiality of client information, which includes making a reasonable effort to ensure privileged data is secure -- even if you are just momentarily lending your device to family or colleagues. Configure these iOS settings for optimal confidentiality:

Snowden Says Lawyers Should Encrypt: In an August 2014 interview, the famous whistleblower warned that all professionals need to encrypt their data. Apple increased its encryption standards in iOS8, which appears to thwart most law enforcement capabilities, *but you must password protect the device*. Go to Settings / Touch ID & Passcode. You should also backup to your computer, not the iCloud, and turn on encrypted backups (in iTunes, select "backup encrypted"). Because the typical 4-digit Passcode is insecure, de-select Simple Passcode. Note, using Touch ID to open your device with your finger is likely not sufficiently safe from a warrant or court order since a fingerprint is non-testimonial and can be compelled.

Your Photos Are Not Deleted Until You Double-Delete: Deleted photos can be viewed on your phone without any hacking or special skills. In iOS 8, if you delete a photo, it is removed from the camera roll and placed into the photo album, "Recently Deleted," for up to 30 days. Open the camera app, hit the photo icon in the bottom left corner, then tap "all photos" in the top left corner, and then "albums" in the bottom right corner. "Recently Deleted" holds all of your unwanted photos for up to a month. Beware.

Hide Photos (But Be Careful): When viewing your camera roll (Camera app / bottom left icon / All Photos), you can press and hold a photo to "hide" it so that it does not appear in Moments, Collections, Years (the main camera roll). However, be aware that "hide" will not remove the photo from any photo albums you have made.

Your Text Messages Are Also Going to Your iPad: When you upgrade to a newer version of iOS, Apple automatically sets iMessages to go to all devices using the same Apple ID. This is a problem if you have a family-shared iPad since anyone with access will see your iPhone texts. On the iPad (or other secondary iDevices), go to Settings / iMessage / Send & Receive and check only your phone number (not email addresses).

Prevent Tracking of Your Internet Searches: if you are concerned that your internet searches on Safari are being tracked by Google, head to Settings / Safari / Search Engine and select DuckDuckGo (note: Apple may still collect your data).

Limit Tracking of Your Internet Viewing: for Safari users, go to Settings / Safari and turn on Do Not Track and Fraudulent Website Warning.

Be Careful With Private Browsing: In prior versions of iOS, when you exited Safari while using Private browsing, it would remind you to close the webpage. In iOS8, however, it does not. After you finish private browsing, you must close out the window otherwise the next person to open Safari will see the last page you visited.

Three Ways to Protect Your Location: Go to Settings / Privacy / Location Services. First, turn off Share My Location. Second, the apps on that long list are monitoring your location -- unless they are essential, turn them to "Never" or "When Using the App." Third, scroll to the bottom of the list to System Services and turn off Location-Based iAds, Frequent Locations, Diagnostics & Usage, and Popular Near Me.

Two Ways to Protect Your Privacy: Under Settings / Privacy, scroll down to Diagnostics & Usage and select Don't Send. Back out to the Privacy tab and select Advertising. Hit "Reset Advertising Identifier" and then turn on Limit Ad Tracking.

Prevent Apps from Listening: Some apps need access to the microphone (*e.g.*, Google Translate, Shazam) whereas other apps seemingly want access without a real purpose (*e.g.*, Instagram, Florida 511). Under Privacy / Microphone, turn off any apps that you do not want to be able to access your microphone.

Turn Off Google Maps Tracking: if you rely on Google Maps, be aware that Google tracks your location history. This is not a setting on your iDevice. On a PC or Mac, go to your Google settings webpage. Hit the "Places You've Been" icon to see Google's information. You can then "Manage History."

Auto Delete Texts: Configure Setting / Messages / Keep Messages to delete SMS messages after 30 days.

Two Step Verification: Prevent unauthorized use of your Apple ID by selecting Manage Your Apple ID from appleid.apple/com. Anytime you purchase from iTunes or access iCloud, you will enter your password and the code sent via SMS.

For the hyper paranoid: Concerned that the plane overhead is surveilling you? Just ask Siri, "what planes are overhead?" to confirm they are just commercial flights.

Christopher B. Hopkins *is a partner at Akerman LLP. Send a tip of the jaunty (tinfoil) cap to christopher.hopkins@akerman.com.*