CHRISTOPHER B. HOPKINS

Protect the Privacy of Your Data on iOS Devices

In a recent cell phone privacy case, Carpenter v. U.S., the Supreme Court noted that Americans "compulsively carry cell phones with them all the time" yet, from a privacy standpoint, "there is no way to avoid leaving behind a trail of [personal] data."

Fortunately, for people who own iPhone and iPad devices ("iOS Devices"), you can limit law enforcement, advertisers, and third parties from accessing your personal data. In less than 10 minutes, with this article in one hand and your iOS Device in the other, follow these steps to protect your privacy.

Before delving in, ensure that your iOS Device is operating on iOS 11.x. You can confirm by going to Settings, General, and then tap Software Update. The most important security protection is a passcode. Go to Settings, Passcode (depending on your device, it will be "Touch ID & Passcode" or "Face ID & Passcode"). Make sure Passcode is turned on and Require Passcode is set to Immediately.

Advertisers: To limit advertisers from tracking your information: (1) in Settings, scroll down to Safari and consider turning on all buttons under "Privacy & Security" except "Camera and Microphone Access"; (2) in Settings, go to Privacy and scroll down; turn off all buttons in Analytics but turn on Limit Ad Tracking under Advertising; (3) in Settings/Privacy/Location Services, scroll down to System Services and turn off Location-Based Apple Ads, Suggestions, and all three buttons under Product Improvements.

I'm Handing You My Phone For You to See One Thing We often share pictures or videos by handing our phone to friends. To avoid letting them leave the app and start snooping, go to Settings/General/Accessibility. Scroll down to Guided Access and turn it on. Under Accessibility Shortcut, tap Guided Access. Now, when you hand someone your phone to look at photos, discreetly hit the side (or top) button three times. It will ask for a passcode. Type in a code and then hand over the device. The person will be locked into that app until you enter the code again. They won't know you've locked them out unless they start snooping.

If you have Face ID, you can simplify the process under Settings/General/Accessibility/Guided Access/Passcode Settings and turn on Face ID. That way, three clicks of the side button will lock the app and two clicks will unlock, as long as it sees your face.

Quickly Turn Off Face ID to prevent law enforcement or third parties from accessing your Face ID protected iOS Device by forcing you to look at it, hold the side button and volume down button for a second. The power off / SOS page will appear. Once you hit cancel, your iOS Device will disable Face ID and require a passcode to access.

Snoopers Can Learn A Lot Just By Looking At Your Lockscreen Apps constantly communicate with you through Notifications on your lock screen. However, third parties can access a lot of your information even if your phone is locked. Head over to General/Settings and then Notifications. Tap each app and turn off Allow Notifications. For apps which you want to provide Notifications, consider (a) turning off Sounds and Show on Lock Screen and (b) settings banners as temporary.

Who is Following Me? Most apps do not need to know your location and, when they do, the best setting is "only while using this app." First, under Settings/Privacy, tap Location Services. Weather, maps, and travel apps, naturally, should have access to your location; most others you can turn off. Second, your device keeps track of where you frequently travel; under Settings/Privacy/Location Services, set Significant Locations to "off." Third, in that same area, turn on "Status Bar Icon" at the bottom. This will put an arrow in the upper right corner of your iOS Device to notify you when the System Services are accessing your location.

Who is Looking at My Deleted Photos? When you delete a photo, it is not really deleted. In fact, it is readily accessible. You can avoid embarrassment by going to the Photos app and scrolling to the Recently Deleted folder and"double delete" any image so it is inaccessible without sophisticated software.

Who is Listening? Under Settings/Privacy, select Microphone to see which apps on your phone have access. Apps like Translate, Shazam, and Skype should stay on. You will be surprised at the games and other apps which want access. If you do not dictate into an app, turn off its access to the microphone.

Who is Watching Me? Under Settings/Privacy/Camera, turn off access to the camera to all apps except those which require the camera to function.

Protect Your Texts Your texts and instant messages are surprisingly revealing. First, there is no reason to broadcast when or whether you have read a text. Go to Settings/Messages and turn off Send Read Receipts. Two, if you have more than one iOS Device, your IM may be going to more than just your iPhone (which means someone using your iPad can see your texts). Under Settings/Messages, set Send & Receive so there is only a check next to your iPhone. Third, in that same section, considering turning Keep Messages to something less than Forever.

Web Browser: To clear your website history (and to regain some space on your device), go the Settings/Safari and hit "Clear History and Website Data." For Chrome, go into the app, hit the three circles in the upper right corner, go to Settings, then Privacy, and then Clear Browsing Data.

Christopher B. Hopkins is a member of McDonald Hopkins LLC. To reach him, tape an "X" to your window or drop an email to chopkins@mcdonaldhopkins.com.