TECHNOLOGY CORNER

CHRISTOPHER B. HOPKINS

Protect The Privacy of Your iOS 13 Device

It has been two years since we covered iPhone and iPad security in this column. The risks have only increased while several privacy settings have become more difficult to find. To echo the Fourth District's recent assessment in a real-time cell phone tracking case: "[t]his presents significant privacy concerns." Make sure your device is running iOS 13.x (Settings / General / Software Update) and then check the following:

Apple Is Tracking You: Under Settings / Privacy / Location Services, scroll all the way down to System Services. Location-Based Apple Ads, Location-Based Suggestions, iPhone Analytics, Popular Near Me, and Routing & Traffic should be off. Turn off Significant Locations.

Google Maps Is Tracking You: Open Google Maps and select your profile in the upper right corner. Select Your Data in Maps, then "See & delete activity." Hit the three dots in the upper right corner and then Settings. They don't make this easy, do they? For true security, Location History should be "off" and delete your all Location History. At a minimum, under "Automatically delete Location History," choose "Keep for 3 months."

People Are Tracking You: Under Settings / Privacy / Location Services, check under Share My Location that this setting is off unless you trust the listed Friends.

Apps Are Tracking You: Again, under Location Services, check the long list of apps. Most should be set to never or "while using."

Turn Off Facebook's Facial Recognition: In the Facebook app, select the three lines in the bottom right corner. Scroll down to Settings & Privacy and hit Settings. Under Privacy, select Face Recognition and hit "no" to turn it off.

I See You When You Opened My Email: If someone sends you an email with an image, they can tell when you opened that email (it's called a read receipt). When you open the image, it remotely loads the image from the sender's server which then reveals when you opened the email. Gotcha! To prevent this intrusion, go to Settings / Mail and toggle Load Remote Images to off. If an email contains an image you want to see, just click the banner at the top when you open the email.

I See When You Opened My Text: Under Settings / Messages, turn off "Send Read Receipts."

I See You Are Not in Your Office: Why broadcast that you are out of the office? Turn off "sent from my iPhone" under Settings / Mail / Signatures (leave it blank). There is still another trick. When sending a reply, your email will be entitled "Re:" when you reply on a mobile device whereas it will be "RE," with a capital E, if you are logged in via computer. So an email which is entitled, "Re: [title]" is coming from a handheld device. When it matters, you can manually capitalize the letter "e" to prevent leaking that information.

AirDrop: Are you wasting battery and creating a security risk by constantly broadcasting an open AirDrop signal? In Settings / General / AirDrop, select Receiving Off.

Are Photos Revealing Your GPS Location? By default, your device inserts location data into your photographs which permits someone to find you if, for example, you post that picture on social media. Under Location Services, scroll down to Camera and set to "never."

We Can See Your Deleted Photos: Anyone with access to your device can view recently deleted pictures. Open the Photos app and scroll down to find your "Recently Deleted." Open that folder and choose Select and Delete All.

Access to Your Camera, Microphone, Bluetooth: Under Settings / Privacy, check these categories to see which apps have access to see, hear, and connect. Many apps over-reach (e.g., why does LinkedIn need access to your microphone?). Shut them out. If you need that feature while using the app later, it will notify you.

Keyboards: While you love to send GIF and Bitmoji images, those services may be able to keylog what you type because you granted them "all access." Make sure you know which apps can read your texts under General / Keyboard / Keyboards. Delete anything which is unfamiliar.

Are Text Messages Going to Other Devices? Are iMessages being pushed to other devices on your Apple account? Maybe. To keep your chats private, make sure Settings / Messages / Send & Receive is set to your phone only and no other devices or email.

Health: Unless you intended an app to access this feature, only Health should be listed under Settings / Health / Data.

....

*Christopher B. Hopkins handles privacy and cybersecurity matters with McDonald Hopkins LLC (**chopkins@mcdonaldhopkins.com**).*

Judge Melanie Surber Robing Ceremony

Friday, March 27, 2020
4:00 PM - 5:00 PM
Palm Beach County Courthouse
205 N Dixie Hwy
Courtroom 11A
West Palm Beach, FL 33401