iPhone Security for Legal Professionals

Anne Haag
Practice Management Advisor, Chicago Bar Association
Bar Leadership Institute
March 13, 2019
The Basics & Customization
This applies to all models of the iPhone prior to the Xs and Xr. These models have an expanded screen. They do not have a home button, and charging is done wirelessly. They still have the buttons on the side, and have some features that we aren’t going to get into here (for example, Face ID).
Apple IDs are the keys to the Apple world. You probably already have one – they prompt you to create one when you first start up your iPhone. You’ll want to use your primary email address, and a secure password. They don’t bombard you with notifications, but it’s where they’ll send receipts from the App Store and important account updates. It’s also your key to the cloud.

Change, recover, update, etc. your Apple ID here: https://appleid.apple.com

It’s important to know your Apple ID, and to be able to login to your account easily. We’ll see why shortly.
A lot of the apps that come preinstalled on the iPhone aren’t the apps you use most often, if ever. To reorder your apps, hold down one of the app icons until they start to shake. You can now move apps around by dragging them with your finger. You can also change the four that always remain in the dock on the bottom. You can delete apps that have x’s in their top left corner by tapping the x. You can also group apps into folders by hovering one app over another that you want it to be grouped with. I have a folder that contains all the apps that I don’t use but can’t delete, just to cut back on clutter. To drag apps between screens, just drag them to the right or left side of the screen edge.

You might have to play around with this a bit before you have it down. Getting the apps to go where you want them to go isn’t a perfect process and frustrates a lot of people. Just keep trying until you get it.

Accidentally delete an app, or have an app ‘disappear’ from your phone? Just open the App Store, type in the name of the app you deleted, and redownload it.
There are 4 types of notifications: pop-ups (top left), banners (top right, the bar on the top of the screen), sounds, and badges (top right, the red circles that display by certain apps). Banners expand to peek notifications (top middle) if you click on them. These are all audio/visual cues tied to the different apps on your device. They’re designed to let you know when something needs your attention or when there’s been any recent activity in that app.

Notifications behave differently in each app, but they all have two things in common:

1) they can help you keep up with everyday tasks and responsibilities,
2) they can drive you up a wall.

There’s good news though! You can really tailor your settings.

There are two main setting types to consider when thinking about notifications:

1) Notification types – you can control what types of notifications are shown for each individual app, or mute them altogether, app by app
2) Privacy – you can control how much information is provided in a notification (the bottom picture shows what a full notification preview looks like, versus what that same notification looks like when you’ve activated some privacy settings)

Go to the next slide to see how to activate these settings.
First, find the Notifications menu. It’s on the first screen that pops up when you open your settings app (above left). Once you open the Notifications menu, you’ll see a list of all your apps (above right).

The privacy settings are at the very top, where it says “Show Previews.” If you tap it, you can select “Always,” “When Unlocked,” or “Never.” If privacy is a big concern for you, select “Never.” If someone sends you a text, the contents of that text will only be visible when you open the Messages app to read it.

To tailor other notification settings, you have to go app by app and select which kind of notifications you want to receive for that app. For example, I turned off banner notifications for all apps, because I didn’t like the intrusion when I was trying to focus on something else on my phone.
Want to go one step further? Do Not Disturb is a great setting that you can activate or even schedule during certain recurring timeframes. Do Not Disturb mutes all notifications without having to actually turn off your phone. You can also tailor your settings so that you can still receive calls, or you can receive a call if a person calls you repeatedly. You get the peace of turning off your phone without losing its functionality or having to worry about emergencies that might pop up.

You can activate this from the settings menu (above right), or you can swipe up on your lock screen and select the moon-shaped symbol (above left).
The iCloud is Apple’s cloud storage space. It’s also the key to being able to utilize features like “Find My iPhone” in emergency situations (more on that in the security section). Ideally, the apps you care about are automatically backing up to the cloud whenever you connect to WiFi without you even having to think about it.

To view the iCloud menu (above right), open your settings, select your Apple ID at the top, and hit “iCloud.” Here you can see how much storage space you have, and what is taking up the most space presently. You can also get more storage (“Manage Storage”). You can also see what apps are backing up to the cloud. Apps that are backing up are toggled on. In the above photo, the only app that isn’t backing up to the cloud is the Mail app.

To see when your phone was last backed up, return to the Apple ID menu and select your device from the list of devices at the bottom. If iCloud backup is turned on, directly underneath it you will see the date of the last iCloud backup.

NOTE: I typically tell lawyers to consider not backing up their Mail to iCloud. The most sensitive client information they have on their phone is likely contained there. They also in all likelihood have a different way of accessing their email if their phone gets stolen – it’s not totally dependent on their phone. It’s a security risk they can avoid by just not backing it up.
Security Considerations
Updates are Apple’s way of patching any holes in the OS that might have been noticed by or vulnerable to hackers, so it’s really important that you keep it up to date.

To update your phone or to make sure no new update is available, go to settings → General → Software Update. If an update is available, you’ll see a red circle (above right) and have the option to install it. Of course, the easiest way to stay up to date is to just install the update as soon as Apple tells you it’s available.
If you misplace your iPhone, iPad, iPod touch, or Mac, the Find My iPhone app will let you use any iOS device to find it and protect your data. It will help you locate your missing device on a map, remotely lock it, play a sound, display a message, or erase all the data on it. If you have your phone backed up appropriately (see the slides about iCloud), this should not be a daunting prospect.

For missing iOS devices, Find My iPhone also includes Lost Mode. Lost Mode locks your device with a passcode and can display a custom message and contact phone number right on the Lock Screen. While in Lost Mode, your device can keep track of where it has been and report back so you can view its recent location history, right from the Find My iPhone app.

In order to successfully use Find My iPhone, here’s what you need:
- To have your data backed up to the iCloud
- To be able to use your Apple ID to login to www.icloud.com. If you lose your phone, this is where you’ll go to access Find My iPhone and use it accordingly. I recommend walking through this now, so that you’re confident in your ability to do it easily if your phone gets stolen
  - You’ll also need to use your Apple ID to pull your data down from the cloud if you get a new phone. An Apple store employee will walk you through this, but you have to know your login

NOTE: To turn on Find My iPhone, go to the iCloud menu in your settings, select “Find My iPhone,” and turn it on.
Maximize Password Strength

The go-to password option for iPhones is a 6 digit passcode. However, you also have the ability to set an alphanumeric password. This is by far the strongest option, but your standard “strong password” rules still apply (a mix of symbols, numbers, and letters that has no rhyme or reason).

GrayKey is a program used by law enforcement to break into iPhones, an issue that first gained strong awareness in the public eye after the San Bernardino shooting in 2015. I mention this because if law enforcement has found a way to take advantage of security vulnerabilities in iPhones, it’s reasonable to assume that these same vulnerabilities will also be found by hackers. For this reason, it’s important to have the strongest password you can.

To create a password, or to change your existing password:
Settings → click on your name/account → Password & Security → Change Password → Enter current password → type new password and verify

To create a Touch ID or a passcode, or to update a Touch ID or passcode:
Settings → Touch ID & Passcode → Enter current passcode → this takes you to a menu where you can set your touch ID or change your current passcode; for now, select “change passcode” → type in old passcode → on screen that says “enter your new passcode,” select “passcode options” → you can select “custom alphanumeric code,” “custom numeric code,” or “4-digit numeric code”
You can set your phone to automatically wipe all content after 10 failed login attempts. I’m not sure that this is necessary for every iPhone user, but you should know that the option is there. Again, this should not be a daunting prospect if you have your phone backed up properly.

To activate this setting:
Settings → Touch ID & Passcode → Enter current passcode → Find “erase data” on the menu and toggle on
Avoid Opening Unknown Links

- In ads, via text, or via email
- If you don’t trust the look of it, don’t open

To help avoid opening unwanted links, and to prevent them from popping up in the first place:
Settings → Safari → make sure the following options are activated: block pop-ups, prevent
cross-site tracking, fraudulent website warning, and ask websites not to track me.

You can also block cookies, but know that this may influence the ability of certain websites to
function. You could always activate it, then turn it off if it becomes an issue as you’re using
Safari down the road.
First and foremost, you should delete an app if you have any reason to doubt its reputability. However, you should also reconsider giving apps access to things like your camera, photos, or microphone. An app typically asks for these permissions when you first open it (above left). A major thing to consider is location services. A lot of apps rely on location services to work properly (Google Maps, for example). A lot of apps really take advantage of this though, and might be collecting your location information at many points throughout the day. For a truly terrifying read about this, check out this article: [https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html](https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html)

To see what apps have access to your microphone:
- Settings → Privacy → Microphone
To revoke access, just toggle off.

To see what apps have access to your camera:
- Settings → Privacy → Camera
To revoke access, just toggle off.

To see what apps are using Location Services:
- Settings → Privacy → Location Services
Your options here are “while using” and “never.” To adjust, you have to go app by app (unless you want to turn off Location Services altogether) and select which option you want.
Siri often asks for verification when you access it from your locked screen before allowing access to contacts, photos, etc., but people have found workarounds to bypass the passcode altogether. You can turn off Siri altogether, or you can set it so that you can still use Siri, but only when the iPhone is unlocked.

To turn off Siri when phone is locked:
Settings → Touch ID & Passcode → enter passcode → under “allow access when locked,” make sure Siri either 1) doesn’t appear here at all, or 2) is toggled off.

Your Siri settings will determine which one of these two options appears, so don’t panic if you don’t see a Siri option here at all.
AutoFill saves login/form fill/payment information and loads it when appropriate as you browse the web. This can be really convenient – your shipping address and CC information pops up automatically when you go to buy something online, your login loads automatically when you go to login to a website. However, if a hacker gains access to your phone and you have all this information saved to AutoFill, they also gain access to all of that information.

To turn off autofill in Safari:
Settings → Safari → AutoFill → make sure all options are off
Two-factor authentication is a security measure that makes it twice as hard for someone to break into your Apple account. Essentially, it makes you login to your account in two ways: with your standard username/password, then with an additional source (typically a code that is texted to your cell phone). You can activate it for your Apple ID. I have it set up so that anytime I try to login to my iCloud account from a new location, I have to verify my identity with a code that Apple texts me.

To set up two-factor authentication:
Settings → click on your name/account → Password & Security → Two-Factor Authentication → your phone will walk you through setting it up
You want your screen to lock automatically after a set amount of time. This way, if you walk away from your phone, no one can have access to your information by simply picking it up.

To make sure auto-lock is on:
Settings → Display & Brightness → make sure Auto-Lock is on or tailor your specifications
A secure messaging app is a more secure way to communicate. I recommend this *especially* over Facebook’s Messenger app, or What’sApp. Signal is a great, free option. All communications that take place within the Signal app are encrypted end-to-end. They aren’t stored on servers anywhere, so minimal information about you or the people you’re communicating with is saved.
Use a VPN

VPN stands for Virtual Private Network and is an alternative way to access the internet that doesn’t involve the risks inherent in using public WiFi networks.

The most important thing you need to know about a VPN: It secures your computer's internet connection to guarantee that all of the data you’re sending and receiving is encrypted and secure. If you are ever on a network that you don’t personally manage (at the airport, a coffee shop, etc.), you should be using a VPN to secure all the information you are transmitting over the internet via your phone.

Once you pick a VPN, you can add it to your device by going to Settings → General → VPN → Turn VPN on → Add VPN configuration.

Private Internet Access is a popular VPN service that encrypts your connection and provides you with an anonymous IP to protect your privacy.
Touch ID is a very common tool used to access your iPhone. Face Recognition is a method available in the new iPhone models that actually uses your face as a passcode. These tools are fun, because they make users feel like they’re living in an episode of the Jetsons.

I’m not willing to say that these are inherently bad forms of identity verification that you should avoid using. I think it’s a more complex issue than that. However, I will say that both methods make me uneasy. Ultimately, you’re handing over a lot of personal information.

The tech world has expanded so significantly over the past two decades that it’s hard to wrap our minds around. Technologies that were unfathomable in 2000 are the status quo less than 20 years later. iPhones are everywhere, and I don’t see that changing anytime soon. However, these technologies have all been developed by companies that value profit over privacy. Until regulations catch up with the landscape, I think it’s wise to err on the side of distrust, especially for anyone working with sensitive or confidential information. For everyone else, it’s up to you to weigh the pros and cons and determine your own privacy thresholds.
Questions?

Contact Info:
Anne Haag
Practice Management Advisor, Chicago Bar Association
ahaag@chicagobar.org
312-554-2059