Privacy on Your iPhone & iPad

Most of us have long assumed that we had some basic *Right to Privacy*. Now, some long-established precedents upon which privacy assumptions were based have been reversed at the Federal level, and State laws are in conflict. It's up to each of us to protect ourselves while our *Privacy Rights* remain unsettled.

This checklist is intended to help us set up our iPhones & iPads so our digital lives are as private as possible, and to minimize the risks of our data being used against us and others.

iPhone & iPad Increased Risks

iPhones and iPads gather more of our data and allow more tracking than do Macs.

It's important to configure Settings appropriately to preserve any level of privacy.

General Guidelines

- Do not assume that what you do, say, or write is private or protected if it conflicts with the laws of any state, not just your own.
- Avoid online discussions of contentious issues if you don't want to be targeted by political extremists or law enforcement.
- Avoid using Apps which feed data brokers, Google, Facebook/ Meta and their subsidiaries, and any Apps with unwarranted location tracking.
- The Federal Government has warned against using Period-tracking Apps.
- Use a search engine other than Google — one that won't save your searches or hand them over to law enforcement.
- If you use Apple's Safari browser, enable Private Relay (see below).
- If you use another browser, consider a VPN to protect your online activity from being monitored by your Internet Provider and others.
- Do not use the Chrome browser. It was designed by Google to collect data.

iOS Settings

The following settings are based on iOS 15 for iPhone, but most also apply to iPad.

These items are controlled from within the **Settings** App of your device. We'll take them in order from the top of the Settings' first screen….

APPLE ID > ICLOUD

- Keychain: use it if you don't have another Password Manager that you prefer.
- Private Relay should be turned On if you're not using another VPN, but it only protects Safari your browsing, not 3rd party browsers or Apps.
- Hide My Email: enable and use for communications you may want to later abandon or not have traced back to your Apple ID after you stop emailing them.
- iCloud Drive: what you store there may or may not be encrypted. Backups are, but most other stored items are not encrypted, and Apple will open your account if served a search warrant.

CONNECTION TYPES

- **Wi-Fi** can be on when Airplane Mode is On. Must turn Wi-Fi off separately in Settings to be sure it can't locate you.
- **Bluetooth** can also be On with Airplane mode unless turned off in Settings.
- **Cellular** is turned Off by Airplane mode.
- **Personal Hotspot** allows connection through your iPhone by others. If activated, use a good password, and only allow people you really trust.
- **VPN** will appear if you have one installed, but it can be disabled without deleting it. Be aware of when it's On/Off.
- GPS cannot be turned Off completely except maybe by powering down the phone. iPhones are intended to be findable with Find My even if it turns Off due to low power. *Leave your iPhone at home if making a trip you don't want logged!*

GENERAL

- AirDrop: if enabled at all, set it to: Contacts Only.
- VPN & Device Management: can enable or disable multiple VPN Apps, but enable only one at a time to avoid conflicts between them.

SIRI

- **Ask Siri** (top section) can enable or disable Siri's availability.
- Delete Siri data from Apple servers periodically.

FACE ID/TOUCH ID & PASSCODE

- Unlock and scroll down to "Allow Access When Locked" and turn it all OFF. It will still instantly be accessible when you unlock with Face or Touch, but not available to anyone who can't unlock your iPhone.
- Use a passcode that's Alpha-numeric so that others can't even tell how long it is (as they canwith numeric-only PINs).

EMERGENCY SOS

- Review what you show and who you list as contacts, keeping in mind this is available to anyone handling your device, even when your iPhone is locked.

PRIVACY

This major section includes which apps can activate your camera and microphone, or view your calendar and contacts, as well as location information.

- **Location Services** main toggle at the top needs to be On for the iPhone to work properly, but it can be turned Off completely in an emergency.
- **Location Services** can be enabled or disabled for each App that is able to use Location data. You need to enable/disable each App in the list as appropriate, setting it to “while using app” if it needs it, otherwise set to “Never”.
- **Tracking** has nothing to do with location; it’s about keeping track of your online or app-based activities on the iPhone, what you do with your iPhone. You do not need to let Apps even ask you to Track your activities. However, it can be interesting to see which apps do ask you for permission to do it. Turning this Off does not assure that no app will track your activity, but Apple says they will remove apps that break this rule. They may try, but some rule-breakers remain.
- *Privacy of your iPhone’s Data sources* such as your **Contacts, Calendar, Photos, Mic** and **Camera** - basically the iPhone’s built-in data repositories of your private stuff. For each of these, you can check and see which apps have access to them and you can turn that access Off or On here. Be particularly careful about allowing Apps to read your Contacts, Photos, and Calendar, and also about which apps can capture data from your Mic & Camera.

PASSWORDS

- Follow up and fix all *Security Recommendations* regarding passwords.

MAIL

- Privacy Protection: enable this to reduce the amount of feedback mail senders get automatically about what you do with their emails.
- Preview: give yourself a Preview of as many lines as you can so you see more of the message before fully opening it.
- To & CC labels: enable so you have info about how email is addressed to you.

MESSAGES

- Text Message forwarding, allow only your known devices, or remove a device from your list.
- Filter Unknown Senders so they go to a separate list if not in your Contacts.

PHONE

- Calls on other devices might be best left Off if there’s any risk of someone else using your other devices when you’r not there.

FACETIME

- It’s now possible to FaceTime with non-Apple devices, but these FaceTime connections lack the encryption and privacy available when using only Apple.

SAFARI

- Choose Duck Duck Go over Google as Search Engine if you want privacy.
- Block Popups: On is good idea.
- Extensions: research their privacy policies before using any extensions.
- Privacy & Security: Turn them all On *except for blocking all cookies*. (You can do that in an emergency if there's an immediate threat.)
- Clear History & Website Data: click this periodically to clear cookies and caches.
- Settings for websites: Deny Camera, Mic, Location permissions unless a site has special features which require these. Very few have any valid use for them.

WEATHER

- Weather doesn't need Location to show saved cities.
- The Weather Channel is a known location data collector & reseller, so don't give their App permission to use it if you can avoid it.
- Reset your identifier periodically.

HEALTH

- Check what's able to see Health data. No need for Messages see Heart Rate.

THIRD-PARTY APPS

- Check Apps' settings for anything you don't understand or seem suspicious.
- Millions of Apps have different options that aren't standard across the Settings described above. Vet their Privacy policies in Apple's App Store before deciding to download the App.

Closing Reminders

- Empty your browser cache and history regularly in Settings > Safari.
  It won't happen by itself.
- Be aware that any website you visit can see your device while you're connected to it, and most sites will collect and save device data, as well as anything you type into any field on their pages, even if you never click on Submit or Save.
- Social Media posts are never private. Don't post what you wouldn't want seen and used by platform employees, law enforcement, or potential opponents.

Apple advertises that Privacy is built into all its stuff, but mostly it's optional and depends on our choices in Settings. Apple's default settings are usually designed for *Convenience* rather than *Privacy*.

IT'S UP TO EACH OF US TO SAFEGUARD OUR OWN PRIVACY.