Your Privacy & Your Mac

For most of our lives we've assumed that we had some basic *Right to Privacy*. Unfortunately, long-established precedents upon which Privacy assumptions were based are now being reversed or challenged at both the Federal and State level.

So, it's now up to each of us to make sure our privacy is protected as best we can. This checklist is intended to help us set up our Macs so our digital lives are as private as possible, and to minimize risks that our data might be used against us.

New Legal Risks

For half a century, federal courts recognized *Privacy* as a right under a *Liberty clause* in the US Constitution. The Supreme Court has now overturned a ruling which relied on that, raising doubts about any right to privacy.

New and proposed laws in some states allow civil suits against anyone for aiding someone who breaks a state law even if those actions happen out-of-state.

Your data might now be used to target not only you, but also as evidence *against whoever you assisted!*

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 a different browser, consider using a VPN to protect your online activity from being monitored by your Internet Provider and others.
- Do not use the Chrome browser or a ChromeOS for computing. Chrome was designed by Google to feed data to Google.

Mac System Preferences

The following settings may help you keep your Mac data and your online activities on your Mac more private.

All of these items are set in the **System Preferences** App on your Mac.

- Apple ID > iCloud > **Private Relay**: Turn it On if you use Safari as your browser and don't have a separate VPN installed. This can hide your IP address and online browsing from your Internet Service Provider, who otherwise may capture and sell this information to data brokers or provide it to law enforcement.
- Also in iCloud > **Hide My Email** allows you to use a unique email when signing up for any service without revealing your Apple ID email, and you can disable these addresses at any time so they no longer connect to you.
- Siri > **Delete Siri & Dictation History** from Apple Servers periodically, just like clearing your browser cache. Stuff on Apple's servers is not always private.
- **Wallet & Apple Pay** includes your name and address on-file with Apple. If you want to use some untraceable form of payment for any goods or services which might raise legal issues, do not expect Apple Pay to hide your identity.
- If you use **Mac Accessibility** features such as **RTT** for phone calls, be aware that those conversations create a saved record of your communications.
- **Internet Accounts**: Disable or delete any accounts you no longer use.
- **Extensions**: check any you might have which rely on remote connections, as these could be recording some of your computer tasks or browsing on a server.
- **Users & Groups**: turn the Guest User OFF and make sure that each active account requires a login password. Verify the reason for any Login Items which are enabled, otherwise disable them. Automatic login should be turned OFF.
- **Sharing**: turn off everything you didn't know you were sharing or don't understand. You'll get a warning if something won't work with Sharing Off. (By the way, this is also where you name your Computer to set how it appears in your Apple ID list of devices or on your Wi-Fi network.)
- **Security & Privacy** has 4 tabs, starting with **General**: set this to require your password very quickly after either sleep or the screen saver kicks in.
- Tab 2, **FireVault** is the best encryption you can have on your startup disk/SSD.
- Tab 2, **Firewall**: turn it On with default settings. If it's already On, leave it alone.
- Tab 3, **Privacy**: numerous items are controlled here:
    1. Location Services — probably good for your Wallet, but remember to turn Safari OFF before visiting any website you wouldn't want to track you to your physical location. Wi-Fi alone might disclose your location fairly accurately.
    2. Contacts: unless you have a very good reason, do not allow third-party (non-Apple) Apps to have access to your Contacts.
    3. Calendar - unless you have a very good reason, do not allow third-party (non-Apple) Apps to have access to your Calendar.
    4. Reminders - allow only if you want to be reminded through that App.

5. Photos - allow only apps with which you need to use Photos. If you have social media apps and use Photos with them, reconsider…. (*see below*)
6. Camera: disable for all apps where you don't intentionally use the camera.
7. Microphone: disable for all apps where you don't need to talk to the App.
8. Input Monitoring: this basically enables *key logging*, which can be a huge security hole. If you see any apps here, think hard about how you got them and whether you want them tracking your keyboard use — letter by letter.
9. Full Disk Access: enable only utilities which must perform disk functions on your drive, such as backups, malware-protection, or disk cleaning. All others apps should have this turned Off.
10. Files & Folders: scan for anything you don't recognize. Disable any you don't want reading or manipulating your files.
11. Screen Recording: this needs to be turned ON for Zoom if you want to *Share Screen* during meetings, even if you don't want it recorded. However, disable all Apps which don't need to "see" your screen's image.
12. HomeKit: enable only apps for your known smart devices.
13. Bluetooth: enable only Apps for your physical bluetooth devices.
14. User Availability: nothing needs enabling for your Mac to work normally.
15. Automation: may appear depending on which Apps you use that do interactive scripting (*i.e.* Shortcuts or Apple Script). Leave it alone for any apps you recognize and use, otherwise disable them.
16. Analytics & Improvements: I would hesitate to let third party developers collect data in the background on how you use their Apps.
17. Apple Advertising: Apple just does this. You can look at what they obviously use to target you, and you can disable Personalized Ads with the checkbox.

Closing Reminders

Empty your browser cache and history regularly; this 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 collect and save device data, as well as anything you enter in any field on their pages, even if you never click the Submit or Save buttons.

Social Media posts are never private. Don't post what you wouldn't want seen and used by platform employees, law enforcement, or other potential opponents.

Apple advertises that Privacy is built into all its stuff, but most of that is optional and depends on our choice of Settings.

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