

ANDROID CONFIGURATION GUIDE

Configure Android to Harden it from Attacks and Reduce Tracking

FOREWARNING

This guide is based on Android 10. Android 10 introduced significant changes to settings, providing improved controls over app permissions. Since only 10% of the Android install base is eligible to run Android 10, chances are your device is using an earlier version, so some or all settings may not be available. Try to take these recommendations and do with them what you can with the settings you have. **Both for security reasons and improved privacy controls, if your device does not support Android 10, you should consider an upgrade.**

Some manufacturers also create custom settings menus that do not follow Google's settings menu format. **While all settings should be present if you are running Android 10, they may not be in the same place as described here – use the search bar to find hard-to-find settings.**

Also, Google places a few privacy controls within your Google Account settings, vice at the device level. Android 10 has significantly improved this situation, with most, if not all, of these settings accessible from your device settings menus. **However, when you are done with this guide, you should also complete the [Google Account Settings Guide](#), found in the [Privacy Settings Checklist](#).**

OVERVIEW

Altogether, this guide will help you to significantly protect both your privacy and your data. If you don't care to do everything, that's your call, but **at least complete [Location](#), [Ads](#), [Activity Controls](#), and [Usage & Diagnostics](#).**

A handful of settings can go a long way to making your device both much more secure and more private.

This guide also seeks to balance usability with privacy and security. **For most users, changing these settings will not impact your use.** In instances where changes might impact some users, it will be explained. While everything here matters, red stars (*) denote **critically important settings for privacy.**

All Android settings (but not application-level settings) can be accessed from the Settings application on your device

(swipe up for the app tray and select settings). Open it, and get started:

LOCATION

Open the **Settings App**, scroll down and tap **Location**.

**** Location Settings.** Location settings are ~80% of your device privacy, or lack thereof. Treat anything enabled with extreme suspicion. **Most people can completely disable location on their tablets without any impact to usability.** You can (and should) do that by **sliding the top slider to off, but should still go through each setting on this menu and toggle it off** – Google appears to still collect your location and related data in some situations if you have not toggled everything off completely. On this menu, it is best to work bottom-up, tap **Advanced** to expand the menu items:

- **Google Location Sharing:** **off.** Unlike Apple's version of this capability, Google does not seem to handle location sharing privately. While its policies and explanations are bit murky on this topic, Google seems to have access to location information if you share it with others, so avoid enabling this if you can.

- *** Google Location History:** **paused (off position).** If you completed the Google Account Settings Guide, this will already be paused. This is Google's recorded history of your location information.

- *** Google Location Accuracy:** **off.** Earlier versions of Android may give you three choices of accuracy, you want device-only. When enabled, Google collects detailed information on surrounding Wi-Fi networks, cellular towers, Bluetooth devices, and more, which is used to fingerprint and track your devices. When disabled, your device only uses local information to orient itself (your GPS receiver) and does not transmit information to Google to find your location.

- **Emergency Location Service:** **on.** This is only used in an emergency and is safe to leave on. Though turning it off will probably not prevent emergency services from getting an accurate location for you (your cell phone provider also sends your location based on tower information).

- **** Wi-Fi and Bluetooth Scanning:** both off. Like Location Accuracy, except these settings expand access to detailed Wi-Fi and Bluetooth information for the apps you use (and the companies behind them).

- **** App Permission: review and select carefully.** Android 10 introduced the choice of “Allowed only while in use,” and this should be the most you allow any app – even navigation and ride-sharing apps work well with this setting (vice always on). For earlier versions of Android, you only have two choices: always or never. With these poor choices you should be incredibly careful about what apps you grant full-time access to your location (OsmAnd is OK). You should also consider keeping even navigation apps you use regularly set to never and allow location access only as needed.

- o **Default Apps:** By default Android will allow always-on access to Google, Google Maps, Google Chrome, and possibly other apps if enabled by your phone’s manufacturer. **Neither Google nor Google Chrome require your location to function effectively – set them to never/denied.** Google Maps, if you decide to continue to use it, will function well with only-while-in-use access.

Next, return to the **main settings menu** and tap **Privacy**.

ADS (PRIVACY)

**** From the Privacy menu, tap Advanced** to expand the bottom menu item. **Select Ads and toggle on “opt out of ads personalization.”** Tap OK to confirm. This denies use of personal information, like your location, to advertisers.

Now, tap **“Reset Advertising ID”** and confirm. You should do this regularly.

Next, return to the **Privacy** menu.

ACTIVITY CONTROLS (PRIVACY)

From the **Privacy** menu, tap **Activity Controls**.

If you completed the Google Account Settings Checklist, you can skip this section. If not, go through and un-check/disable/pause all items.

When you are done, return to the **Privacy** menu.

USAGE AND DIAGNOSTICS (PRIVACY)

From the **Privacy** menu, tap **Usage and Diagnostics**. **Toggle it off.**

Return to the **Privacy** menu.

AUTOFILL SERVICE FROM GOOGLE (PRIVACY)

From the **Privacy** menu, tap **AutoFill Service from Google**.

Review each item – recommend you disable all items and delete all stored information (you will probably need to keep payment information for your Google Play account). If you completed the Google Account Settings Checklist (or if you plan to), then you don’t need to review Personal Info. This is your public Google profile. If you have not reviewed it yet, then delete everything under Personal Info except your name, date of birth, and email. Tap each of these to restrict them as much as possible (most allow Only Me).

When you are done, return to the **Privacy** menu

PERMISSION MANAGER (PRIVACY)

From the **Privacy** menu, tap **Permission Manager**.

Here, **review each item** (Body Sensors, Calendar, Call Logs, Camera, etc), **and deny access to any app that does not seem to have a good reason for accessing this data.** If you don’t use OK Google, you can deny the Google app access to things like Contacts without impacting your routine usage. Be particularly careful about granting apps access to Contacts and Call Logs:

- **** Contacts. Sharing contacts with an app is dangerous.** Many apps abuse this privilege by uploading your entire contacts list to the parent company and sharing or selling them to advertisers. Not just the names, but the numbers, emails, and everything else. **Avoid sharing them with social media applications.** Sharing them with Signal Messenger is okay though, along with most privacy-first services (e.g. ProtonMail).

- **** Call Logs.** Like contacts, call logs can tell a lot about you – who you call and when, what services you use, where you work, and much more. **Be careful with granting access to anything other than the phone app.**

When you are done reviewing everything, return to the **main Settings menu**.

SECURITY

Next, **tap Security** from the main Settings menu. We will work through each item:

Google Play Protect.

- **Scan device for security threats:** **on**.
- **Improve harmful app detection:** **off**. This sends diagnostic data on your apps to Google.

Security Update. Check for and install any available updates.

**** Screen Lock (Password).** The strength of the password you set for screen lock is what stands between someone trying to pull data from your device and your data – it is what encrypts your device. **A strong password is particularly important.**

- **Under Screen Lock, tap Password.** Choose a strong two or three-word diceware password. This is much more secure than a PIN, swipe, or pattern.
- When you have entered and confirmed your new password, **select either “show sensitive content only when unlocked” or “don’t show notifications at all.”** A thief can learn a lot about you without unlocking your device if it shows all notifications.

Fingerprint/biometrics. If fingerprint or another biometric login is available, **enable/use it whenever available**. While not as secure an implementation as Apple’s FaceID/TouchID, this is a good, secure option. It also lessens the pain of entering your new password in all the time.

Smart lock. For maximum security, **don’t use smart lock**. Sophisticated hackers can potentially fool these identification methods to gain access to your device.

Next, return to the main **Settings** menu.

Encryption. As of Android 10, all devices are required to enable encryption by default. Under Encryption & Credentials, it should say “encrypted.” **Older Android devices may not be encrypted by default.** Tap Encryption and enable full disk encryption. Plug in your device – it could take over an hour to fully encrypt and will drain the battery if unplugged.

- If you have an SD card plugged into your device, you should also be able to encrypt it from this menu.

Return to the main **Settings** menu.

SYSTEM

Tap **System** from the main settings menu.

- **Tap Backup.** Backing up your device is up to you (it’s a good idea), but Google doesn’t give you granular control over what gets backed up. Starting with Android 9 (Pie), **Google encrypts your device backups using your device password** (another reason for a strong device password), so Google cannot access your backups/phone content this way. Note that **Google’s backups don’t include your files**; you can keep them safe from a factory reset by always saving files to a cloud drive (preferably a private one like Sync or Tresorit).
- **Tap Advanced and then System Update.** Check to see if you can update your system software and **update if available**.

Return to the main **Settings** menu.

NETWORK & INTERNET

From the main **Settings** menu, **tap Network & Internet**.

Encrypted DNS. **Tap Advanced** and then **Private DNS** (Android 9 and later). **Select the radio button for Private DNS Hostname** and **enter:**

1dot1dot1dot1.cloudflare-dns.com This will enable encrypted DNS for all your phone’s activity through Cloudflare’s 1.1.1.1 service.

Wi-Fi Settings. Next, **tap Wi-Fi**.

- **Tap Wi-Fi Preferences.**

- o **Turn off both** “turn on Wi-Fi automatically” and “open network notification.”
- o If Wi-Fi calling is available on your device, **turn it on here** (you may need to tap Advanced first). If it is not here, try searching for “Wi-Fi Calling” in the search bar at the top. Return to the Wi-Fi menu when done.

- **Tap Saved Networks.** **Review saved networks and forget unused and public networks.** Forget by tapping the network, and then tapping forget.

Return to main Network & Internet menu.

HOW TO TURN OFF/ON WI-FI AND BLUETOOTH

It is a good security practice to turn Wi-Fi and Bluetooth antennas off when you're not using them to prevent fingerprinting, beacon tracking, and some possible device attacks. **You can do this easily at any time by swiping down from the top of the screen and de-selecting the Wi-Fi and/or Bluetooth icons.**

1.1.1.1 APP

If your device is running Android 9 or later, you can enable encrypted DNS ("Private DNS" above) without downloading/using the 1.1.1.1 app. Nevertheless, **the app is great as a fire-and-forget privacy solution if you plan to use the WARP service, which can be comfortably left on all the time and provides improved privacy and security. To use WARP, download the 1.1.1.1 app and turn the slider on.** That is, your internet service provider can no longer see how you use the internet.

The **settings** menu is in the top right, **tap it:**

- You can optionally choose to select/pay for WARP+, which may give you moderately faster internet speeds.
- If you use a separate VPN, you should turn off WARP when using your VPN, but can still use the 1.1.1.1 DNS service.
- WARP is great to leave on all the time. It will hide your internet activity from your internet service provider and will not meaningfully impact your internet speed (WARP+ may even improve it).
- Unlike a VPN, WARP does not hide your IP address from the sites you visit and services you use.

You should change one setting. From the app's settings menu, tap **Advanced -> Connection options -> DNS settings -> Protocol options -> select DNS over HTTPS**. From the DNS settings menu, you can also optionally have 1.1.1.1 block requests for sites with known malware, and/or adult content, by changing the options under "1.1.1.1 for Families."

SIGNAL APP

Go to the Play store and **download the Signal Messenger app** (listed in Play store as "Signal Private Messenger"). See [accompanying guide to configuring and using Signal](#).

GOOGLE ACCOUNT SETTINGS GUIDE

When you are finished here, complete the [Google Account Settings Guide](#) to make sure your Google account is private and secure.

FACTORY RESETING YOUR DEVICE FOR SALE/TRAVEL

If you're going on a trip to a high-risk country (it's best not to bring your device, but maybe we're talking about a "burner" device here), selling/giving away your device, or recycling it, you should first factory reset it. This will wipe all data from the device. To do this:

1) To force a backup of the device: Go to **settings app -> Google -> Backup -> Tap Back up Now**. When it finishes, move on.

2) Disable Find My Device (if enabled). Go to **settings app -> Google -> Location -> Security -> Turn off remotely locate this device**.

3) Back up any local files to the cloud.

3) Reset. Location of reset varies considerably across manufacturers. In **settings app's search bar**, search "**reset options**." Select and tap "erase all data (factory reset)."

If you are doing this for high-risk travel, then set up the device by creating a new Google Account with a different/throwaway email address and follow the above guide to lock it down.

When you return, you can restore from your backup by first factory resetting the device again, and then setting up the device with your normal Google Account. When setting up, restore from your backup.

iOS/iPadOS CONFIGURATION GUIDE

Configure iOS to Harden it from Attacks and Reduce Tracking

OVERVIEW

Altogether, this guide will help you to significantly protect both your privacy and your data. **If you don't care to do everything, that's your call, but at least complete Location Services, Analytics & Improvements, and Advertising. We'll do these first.** Downloading and activating the 1.1.1.1 app is also a quick route to more privacy from your internet service provider.

For iOS/iPad OS devices, unlike many competitors, most operations occur on your device without sending data to corporate servers. Because of this, **a handful of settings can go a long way to making your device both much more secure and private.**

This guide also seeks to balance usability with privacy and security. **For most users, changing these settings won't impact your use.** In instances where changes might impact some users, it will be explained. While everything here matters, **red stars (*) denote critically important settings for privacy.**

All iOS/iPadOS settings (but not application-level settings) can be accessed from the **Settings application on your device.** Open it, and get started:

* LOCATION SERVICES

Open the Settings App, scroll down, and tap **Privacy**. Then tap **Location Services**.

**** Location Services.** Location services are ~80% of your device privacy, or lack thereof. Treat anything enabled with extreme suspicion. **Many iPad users can disable location services (top slider) without any impact to usability.** You may need to occasionally enter an address instead of having location auto-populate. If you use your device for navigation, ride-sharing apps, and a few other legitimate needs, you need to keep this top slider turned on. **If you think you can go without, turn off the top slider and move on – you're done with this section.** If not, continue:

- **Location alerts & share my location.** These are end-to-end encrypted and **OK to use.** Apple can't get this information.
- **Review apps with permissions.** When you tap them, there will be a small paragraph explaining why the app thinks it needs location services. It's almost always an overstatement. In most cases, the company behind the app collects any location data and may sell/share it. They want it enabled.

Default to never, or at most, "ask next time," when in doubt. Navigation apps and other location-driven apps, like ride-sharing, work well with "While using" and don't require "always" access. As an even better practice, you can keep location services off most of the time and only turn it on when you need it.

- o **Apple Maps is a good private alternative to Google Maps or Waze.** When we change some settings below (next and later, under analytics), Apple won't get any information.
- o **Most of Apple's apps (e.g. Find My, Siri), except News and Apple Store, handle your location privately** on-device or end-to-end encrypted (e2ee), which means Apple can't see/access the information.

- **** Scroll to the bottom and tap System Services.** These are dangerous, because they're mostly what is used to report your location, Wi-Fi and Bluetooth information to advertisers. Go through them carefully. Recommendations in blue. For explanations of most of these, visit:

<https://support.apple.com/en-us/HT207056>

- o **Apple Pay Merchant Identification:** **off.** (If you use Apple Pay in brick-and-mortar stores, keep this on)
- o *** Cell Network Search:** **off.** Doesn't affect use – reports cell tower information to Apple.
- o **Compass Calibration:** **on.** If you use your device for navigation, keep this on; otherwise, turn off. Info stays on device.
- o **Emergency Calls & SOS:** **on.** Only used in an emergency to report your location.
- o **Find my iPhone/iPad:** **on.** E2ee - safe to use.
- o **HomeKit:** **off.** If you use HomeKit/Apple Home, it is e2ee – safe to turn on.
- o **Location-based alerts:** **off.** These are for location-based reminders, not things like Amber alerts.
- o **** Location-based Apple Ads:** **off.** Shared with advertisers.
- o **** Location-based Suggestions:** **off.** Shared with advertisers.
- o **Motion Calibration & Distance:** **on.** If you use navigation or fitness trackers, keep this enabled. Otherwise, turn off.
- o **** Networking & Wireless:** **off.** Used to report nearby WiFi/Bluetooth networks, which can be used for fingerprinting. Doesn't affect use.
- o **Setting Time Zone:** **off.** If you travel regularly, it's safe to keep on.
- o **Share My Location:** preference. If you use Find My with family, or send your location to people through iMessage, this is safe to leave on. It's e2ee.

- **System Customization:** ☒. This is handled on-device and not reported to Apple.
- **Wi-Fi Calling:** ☒. Does not impact use of Wi-Fi calling, otherwise used to report your location to cell carriers.
- **Significant Locations:** ☒. While spooky, this information is e2ee and handled on-device. Safe to keep on for use with Apple Maps.
- **** Toggle off all product improvement (iPhone/iPad Analytics, Popular Near Me, Routing & Traffic, Improve Maps).** These don't affect your use and all of them report location information to Apple.
- **Status Bar Icon:** ☒. Provides icon in top left of screen that reports when location is being accessed. Not terribly informative because it's often for local use and your location isn't being transmitted/shared, but still worth keeping on.

ADVERTISING

Return to the **Privacy** settings menu, scroll to the very bottom and **tap Advertising**.

- **** Toggle on Limit Ad Tracking.**
- **Tap "reset advertising identifier."** You should do this regularly. Between limit ad tracking, and changing your location settings, you've significantly reduced tracking, but it's not gone entirely.

ANALYTICS & IMPROVEMENTS

Return to the **Privacy** menu, and select **Analytics & Improvements** right above Advertising.

- **** Switch off all three toggles (Share iPhone/iPad Analytics, Improve Siri & Dictation, and Share iCloud Analytics).** You can see just how much data your device collects for analytics by tapping "analytics data." Your device will continue to collect this information locally, but it will no longer be transmitted to Apple.

GENERAL PRIVACY SETTINGS

Return again to the Privacy menu. Now, review every item (Contacts, Calendars, Reminders, etc) and revoke access to any apps that don't seem to have a clear reason for the information. Be particularly mindful of:

- **** Contacts. Sharing contacts with an app is dangerous.** Most apps heavily abuse the privilege by uploading your contacts to the parent company and sharing and selling them to advertisers – not just the names, but the numbers, emails

– everything. **Avoid sharing them with social media applications, in particular.** Sharing them with Signal Messenger is okay though, and also most privacy-first services (i.e. ProtonMail).

- *** Bluetooth.** Bluetooth information can be used for a lot more than streaming your music. It can be used to uniquely identify and track you. Again, only grant access to apps that absolutely need it to function (e.g. fitness trackers, smart locks). Default to turning it off.

- **Again, review every item, not just these two.**

iCLOUD

From the **main settings** menu, **tap your name/photo/AppleID** at the very top of the menu. **Then tap iCloud. Review which apps back up to iCloud.** You generally want to avoid backing up anything that has sensitive data unless you know it's fully encrypted when backed up.

- **The following are e2ee and OK to back up to iCloud:** Wallet, Health, Home, Maps, Keychain, Safari, Siri, and overall device backup ("iCloud Backup").
- **These are also OK to back up:** Signal, Microsoft Authenticator.
- **These SHOULD NOT be backed up:** Messages, WhatsApp. In both cases, your messages (only iMessages for Messages app) are secure on your device but when backed up to iCloud, they're backed up with your private key that can be used to read all of them.

2FA

Return to the **AppleID** menu with your name at the top. The first item, "Name, Phone Numbers, Email" can be used to update/change your email and information. Next, **tap Password & Security: Ensure 2FA is turned on. If not, turn it on.**

FACE ID & PASSCODE

Return to the **main settings** menu, scroll down and tap **Face ID & Passcode**. Enter your existing passcode.

FaceID/Touch ID: Turn on Face/TouchID for all items in first menu (iPhone/iPad Unlock, iTunes & App Store, Apple Pay, etc).

- Tap **Other Apps and enable for any available app.**
- **In general, whenever an app asks you, or gives you the option to enable or use FaceID/TouchID, the answer should**

always be yes. FaceID/TouchID are very secure, and when you add it (usually with a PIN if unavailable) to apps, it significantly improves the app's security, often adding another layer of encryption to the data within the app.

- (FaceID Only): Ensure "Require Attention for Face ID" and "Attention Aware Features" are turned on.

**** Set a new strong passcode** (ideally: two or three words generated with diceware): **tap blue "Change Passcode" link**, enter your existing pin/passcode, **select blue "Passcode Options" link**, **select "Custom Alphanumeric Code,"** and **type in your new strong passcode.** This is critically important – the complexity of this passcode is the only thing protecting all of your data if your device is stolen or ripped, or someone gains access to your iCloud device backup. It is what encrypts your device.

Next, review items under "Allow Access When Locked:"

- Be very careful about what you allow here, because it's both not encrypted and available to anyone who takes your device.

- **At a minimum: toggle off "USB Accessories" and Wallet.** Allowing access to USB Accessories could let an adversary bypass your device's security.

**** At the very bottom, turn on "Erase Data."** Without this on, your passcode can be guessed infinitely until it's cracked (governments can currently bypass this setting though, so it's not perfect). If your toddler types in 10 bad passwords, you can always restore from your iCloud backup.

GENERAL SETTINGS

From the main **Settings** menu, tap **General**.

First, tap Software Update:

- If any updates are available, tap "Download and Install."
- **Ensure Automatic Updates, at the bottom, is turned on.**

Next, AirDrop: set to contacts only or receiving off. Allowing everyone presents security risks.

AirPlay & Handoff: If you don't use Handoff or don't know what it is, **turn all of these off.**

CarPlay: If you use CarPlay, select your vehicle and ensure "Allow Carplay While Locked" is turned off. This could be used to bypass your device's security.

Background App Refresh: Turn off background app refresh for any social media apps you retain, and any app you don't trust. It will reduce their ability to collect information on your usage.

SIRI & SEARCH

From the main **Settings** menu, tap **Siri & Search**.

- **Turn off "suggestions on lock screen."**

- **For any app with sensitive data**, or that you don't want data being collected about your usage (e.g. messages). **Tap the App and turn off "Learn from this App."**

ITUNES & APP STORES

From the main **Settings** menu, tap **iTunes & App Stores**.
Ensure automatic downloads for App Updates is turned on.

PASSWORDS & ACCOUNTS/AUTOFILL

From the main **Settings** menu, tap **Passwords & Accounts**, then **AutoFill Passwords**.

- **Turn on "AutoFill Passwords" and select your password manager app.** This will let you autofill passwords anywhere in iOS from your password manager.

PHONE (IPHONES ONLY)

From the main **Settings** menu, tap **Phone**.

- **Tap Wi-Fi Calling and enable "Wi-Fi Calling on This Phone".** Follow prompts. It should check if your cellular plan supports Wi-Fi calling without added costs (it has to connect you with your carrier as part of the process), but if it doesn't, you should also check on your own to avoid any billing surprises.

MESSAGES

From the main **Settings** menu, tap **Messages**. **Ensure iMessage is turned on** (at top). If you never again want to send an unsecure SMS message, turn off "Send as SMS."

A note: iMessage and Facetime are both secure and private. Make liberal use of both, especially replacing phone calls you would make with Facetime (you can do just audio if you want). Signal Messenger is even more private, so that should always be your first choice if it's available.

WI-FI SETTINGS/FORGETTING WI-FI NETWORKS

From the main **Settings** menu, tap **Wi-Fi**. Here, you turn off Wi-Fi by setting the slider off (one of three ways, discussed below).

- **Set "Ask to Join Networks" to "Ask."** Auto-joining networks is dangerous because someone can see what networks your device broadcasts (it broadcasts a list of known networks), name one that, and use it to snoop on your activity.

- **Set "Auto-Join Hotspot" to "Ask to Join."** For the same reason.

It's also a good practice to forget public Wi-Fi networks after you use them to make it more difficult to fingerprint your device, and to prevent man-in-the-middle attacks. Unfortunately, iOS does not provide a menu for reviewing remembered networks, *so the only way to do this is while you are still connected to the network. Tap the information icon to the right of the network* (an "i" with a circle around it), and tap **"Forget this Network."**

1.1.1.1 APP

Go the App store, search for, and install/download the free Cloudflare 1.1.1.1 app. **Open the app and turn the slider on.** That's it, really. Your internet service provider can no longer track your internet use.

The settings menu is in the top right, tap it:

- You can optionally choose to select/pay for WARP+, which may give you moderately faster internet speeds.
- If you use a separate VPN, you should turn off WARP when using your VPN, but can still use the 1.1.1.1 DNS service.
- WARP is great to leave on all of the time. It will hide your internet activity from your internet service provider and won't meaningfully impact your internet speed (WARP+ may even improve it).
- Unlike a VPN, WARP does not hide your IP address from the sites you visit and services you use.

You should change one setting. From the app's settings menu, tap Advanced -> Connection options -> DNS settings -> Protocol options -> **select DNS over HTTPS**. From the DNS settings menu, you can also optionally have 1.1.1.1 block requests for sites with known malware, and/or adult content, by changing the options under "1.1.1.1 for Families."

SIGNAL APP

Go to the App store and download the Signal Messenger app (listed in app store as "Signal – Private Messenger"). [See accompanying guide to configuring and using Signal.](#)

HOW TO TURN OFF BLUETOOTH/WI-FI WHEN NOT IN USE

As discussed in the Checkup, it's best to keep both Bluetooth and Wi-Fi turned off when you're not using them because both can be used to fingerprint your device and track you.

In iOS, there are three ways to do this; use whichever one works for you.

1) **Control Center.** Swipe down from the top-right corner of the screen (this even works while the device is locked). The Bluetooth/Wi-Fi buttons are in a small box paired with Airplane mode (a plane) and your cellular antenna (an antenna with waves emanating out of it, if you have one). When they're on, the Bluetooth and/or Wi-Fi buttons are blue. Tap them to turn them off (for Wi-Fi, this only turns it off until the next day).

2) **Siri.** "Hey Siri, turn off Bluetooth." Or, "Hey Siri, turn off Wi-Fi."

3) **Settings.** From the settings app's main menu, Wi-Fi and Bluetooth are both near the top. Tap and turn the slider at the top to off.

FACTORY RESETTING YOUR DEVICE FOR SALE/TRAVEL

If you're going on a trip to a high-risk country (it's best not to bring your device, but maybe we're talking about a "burner" device here), selling/giving away your device, or recycling it, you should first factory reset it. This will wipe all data from the device. To do this:

- 1) **To force a backup of the device:** Go to **settings app** -> tap your name/picture/AppleID at the top -> tap iCloud -> scroll down and tap iCloud Backup -> **tap Back Up Now**. When it finishes, move on.
- 2) **Disable Find my iPhone/iPad.** Also from the name/picture/AppleID menu, just below iCloud, **tap Find My. And turn Find My iPhone/iPad off** (follow prompts). You can't register this device with another account until you have done this (nor can anyone else if you're selling/giving it away).
- 3) **Reset.** From the main **Settings** menu, **tap General**. Scroll to the bottom, and tap **Reset. Then select Erase all Content and Settings**.

If you're doing this for high-risk travel, then set up the device by creating a new AppleID with a different/throwaway email address and follow the above guide to lock it down.

When you return, you can restore from your backup by first factory resetting the device again, and then setting up the device with your normal AppleID. When setting up, it will give you the option to restore from your previous backup.

MacOS CONFIGURATION GUIDE

Configure MacOS to Harden it from Attacks and Reduce Tracking

OVERVIEW

Altogether, this guide will help you to significantly protect both your privacy and your data. **If you don't care to do everything, that's your call, but at least complete Location Services, Analytics & Improvements, and Advertising. We'll do these first.**

A handful of settings can go a long way to making your device both much more secure and private.

This guide also seeks to balance usability with privacy and security. **For most users, changing these settings won't impact your use.** In instances where changes might impact some users, it will be explained. While everything here matters, red stars (*) denote critically important settings for privacy.

All MacOS settings can be found in System Preferences. You get there by clicking the top left Apple menu, then selecting **System Preferences**.

Open it, and get started:

LOCATION SERVICES

From System Preferences, select Privacy & Security -> click the Privacy tab at the top of the window ->

**** Location Services.** Location services are ~80% of your device privacy, or lack thereof. **Most people can disable location services on their Mac altogether and have no impact to usability.** You may need to occasionally enter in a zip code or an address instead of having it auto-populate, it's a small price to pay for significantly better privacy.

First, click the padlock icon in the bottom left and enter your password.

To completely disable location services, uncheck the checkbox at the top next to "Enable Location Services."

If you disabled location services, then you're done with this section. If not, continue:

- * **First, review the apps/services in the box and disable anything that doesn't absolutely need your location.** Uncheck to disable. Siri & Dictation will send location data to Apple if you enable it.
- ** **Next, click the "details" button next to System Services and uncheck/disable the following: Location-Based**

Suggestions, Location-Based Apple Ads, and Wi-Fi Networking. All three of these send location data to Apple that is shared with advertisers and others. Wi-Fi Networking is used to map Wi-Fi networks that can be used for Wi-Fi fingerprinting and tracking. **The others are handled privately** (end-to-end encrypted) on on-device, **and are safe to leave turned on (time zone, significant locations, find my Mac, and HomeKit).**

ADVERTISING

From the same menu as location services, on the left of the window, **scroll all the way down to select Advertising.**

- ** **Check the box next to Limit Ad Tracking.**
- **Click "reset advertising identifier."** You should do this regularly. Between limit ad tracking, and changing your location settings, you've significantly reduced tracking, but it's not gone entirely.

ANALYTICS & IMPROVEMENTS

Next, from the same menu, on the left below location services, click **Analytics & Improvements.**

- ** **Uncheck all three boxes (Share Mac Analytics, Improve Siri & Dictation, and Share with App Developers).**

GENERAL PRIVACY SETTINGS

Again from the same menu under the Privacy tab, now go back and review every item on the left (Contacts, Calendars, Reminders, etc) and revoke access to any apps that don't seem to have a clear reason for the information. Be particularly mindful of Contacts:

- ** **Contacts. Sharing contacts with an app is dangerous.** Most apps heavily abuse the privilege by uploading your contacts to the parent company and sharing and selling them to advertisers – not just the names, but the numbers, emails – everything. **Avoid sharing them with social media applications, in particular.**
- **When you have reviewed every item, continue.**

FIREWALL

Next, click the **Firewall tab** at the top of the window. Click **"Turn on Firewall"** box if not turned on.

FILEVAULT ENCRYPTION

Next, click the **FileVault tab** at the top of the window. If FileVault is turned on, you're good. If not, click **"Turn on FileVault"** box.

This is critically important for your data security. FileVault encrypts your hard drive and protects all of your data.

Recommend: select **"create a recovery key and do not use my iCloud account."** Storing your recovery key in iCloud potentially enables an adversary with access to your iCloud account to unlock your data. Keep the recovery key someplace safe (e.g. encrypted Standard Notes note, printed out and someplace safe... like a safe).

STRONG PASSWORD AND PASSWORD SECURITY

Next, click the **General tab** at the top of the window (still in Privacy & Security).

- **** Set a strong new password.** Use diceware to generate a 4-6 word password and enter it here by clicking "change password." This is critically important – the complexity of this passcode is the only thing protecting all of your data – it is what unlocks the encryption (FileVault) on your data.
- *** Disable automatic login. Ensure this box is checked.** There's not much point in encrypting your data with a small password if you bypass it.
- *** Check require password X minutes after sleep or screen save begins.** Set a reasonable time (15 minutes is good). If you travel regularly with your Mac, set a shorter time (like immediately). Again, you don't want to bypass the protection you just put on your data.

When you're done, click the < in the top left of the window to return to **System Preferences**.

TOUCHID (OR FACE ID)

The Mac used to write this guide was not equipped with TouchID (at this time no Macs support FaceID, but it's likely in the future). If your Mac is equipped with TouchID/FaceID, you should enable it for as much as possible. It's a very secure login method that is virtually impossible to bypass.

You still need a very strong password backing it up (the password is what encrypts your files).

Turn on/manage TouchID by going to **System Preferences -> TouchID**.

SIRI

From the main **System Preferences** screen, click **Siri**.

- If you don't use Siri on your Mac, uncheck **"Enable Ask Siri"** on the left.

- If you do, click the **"Siri Suggestions and Privacy"** box. Go through the applications listed, and for anything with sensitive data that you don't want information sent to Apple about (e.g. Messages), uncheck **"Learn from this App."**

When you're done, click the < in the top left of the window to return to **System Preferences**.

SPOTLIGHT

From the main **System Preferences** screen, click **Spotlight**.

- **Review Spotlight settings.** If there's anything you don't want Spotlight indexing (this stays local, but maybe other people use your account), uncheck it. To not have it index specific directories, add them by clicking the Privacy tab at the top and add them there.

- **Uncheck Allow Spotlight Suggestions in Lookup.**

When you're done, click the < in the top left of the window to return to **System Preferences**.

SOFTWARE UPDATE

From the main **System Preferences** screen, click **Software Update**.

- **Ensure the box that says "Automatically keep my Mac up to date" is checked.**

- **Click the "advanced" box next to this, and ensure every box is checked.** Click ok when done.

- If any updates are available, download/install them.

When you're done, click the < in the top left of the window to return to **System Preferences**.

1.1.1.1 APP

As of this writing, Cloudflare's 1.1.1.1 WARP service was in closed beta testing for desktops. When it's available for broader download/install, it's a good solution to force all of your computer's connections through encrypted DNS and encrypt your traffic so that your internet service provider cannot see what you're up to on the internet.

TURN OFF/ON BLUETOOTH AND WI-FI

Both Bluetooth and Wi-Fi are typically in the menu bar at the top of the screen. Tap the icon and turn them off/on.

If the Bluetooth icon is not in the menu bar, you can add it by going to System Preferences -> Bluetooth -> and checking the "show Bluetooth in the menu bar" checkbox.

FACTORY RESET

Backing up and factory resetting a Mac or PC is much more complicated and time consuming than for a mobile device like an iPhone. For this reason, it's best to just buy a cheap computer if you need a computer when traveling to a high-risk country.

Here are some guides from Apple that will help you along the way (whether you're traveling, or selling/giving/recycling your Mac):

Backing up your Mac: <https://support.apple.com/mac-backup>

Resetting a Mac: <https://support.apple.com/en-us/HT201065>

How to erase a disk for Mac: <https://support.apple.com/en-us/HT208496> (you want to choose secure erase)

THE PRIVACY SETTINGS CHECKLIST

This checklist will help guide you through making your devices and accounts more private, restricting data collection, and stopping the sale of your data.

WHAT THIS CHECKLIST DOESN'T COVER

This checklist doesn't cover the device settings for your primary [iOS/iPadOS](#), [Android](#), [MacOS](#), or [Windows](#) devices. They each have different settings guides to help you get the settings right. It also doesn't cover social media settings, see the [Social Media Settings Guide](#) for detailed instructions on making your social media accounts private. Lastly, to make your browser more private, see the [Firefox](#) or [Brave](#) settings guides.

OVERALL GOAL

The overall goal of this checklist is to guide you through reviewing the privacy settings on the secondary devices you use (e.g. TVs, digital assistants), and the online accounts you have. You might not find all of the settings everywhere, and they just might not exist, but your goal is to reduce the collection, sharing, and sale of your data as much as possible.

Once you have completed this checklist, you want to get into the habit of going through the process of checking settings, requesting opt-outs, and sending do-not-sell requests whenever you get a new device or create a new account.

DEVICE REVIEW

The first thing you should look at is your devices. **If you have trouble finding the settings, search for answers on DuckDuckGo or Startpage.com, something like: Amazon Alexa privacy settings.** As you review devices, you're looking for the following:

- Disable targeted advertising and ad tracking (sometimes called "opt outs" or "personalized ads")
- Disable location tracking and history/logging
- Disable/opt-out of "analytics" or "help us improve your experience" data collection
- Disable/opt-out of the sale of your information
- Disable/opt-out of anything that looks or sounds like data collection (look for trigger words: "log," "record," "collect,"

"store," "analyze," and features that "suggest" things for you)

- Enable two-factor authentication, or additional authentication measures (especially for smart home devices)

Checklist: Devices you should review for privacy settings:

- ☐ Smart TVs, DVD players, even some receivers
- ☐ Media player devices (e.g. Amazon FireTV, AppleTV, Roku, Google Chromecast)
- ☐ Digital Assistants (e.g. Amazon Echo/Alexa, Apple HomePod, Google Home)
 - Settings are usually in the app
- ☐ Amazon Tablets (e.g. Fire), Kindles, and other e-readers
- ☐ Game consoles (e.g. Xbox, Playstation)
- ☐ Mesh or "cloud-enhanced" routers (e.g. Google WiFi)
 - Settings are usually in the app
- ☐ Smart home devices (e.g. Ring, Nest, smart thermostats)
 - Settings are usually in the app
- ☐ Late-model cars with infotainment systems (may need to consult manufacturer privacy policy)
- ☐ Finally, do a walk-through of your house to find any devices you might have missed.

APP SETTINGS REVIEW

Go through each of the apps on your smart phones/tablets and check them for settings related to privacy. Depending on the app, some settings may be on the service's website (see next section). Usually, these settings are inside the app, not in the general settings app for your device. You should review both, because the device's settings app will give you control over things like location and contacts sharing. Be very careful about what applications you choose to give access to your location, contacts, calendar, microphone, camera, photos, and other data on your devices. You should assume that most services requesting this access will collect, misuse, and sell or share it.

Also check commonly used applications on your desktop/laptop (even Microsoft Office collects some data by default).

SERVICE REVIEW

Review websites for services and websites you use. Specific guides for [Google](#), [Amazon](#), and [Microsoft](#) accounts are available on the following pages. It may help to go through password lists, or similar, to identify all of the sites. For each site, you want to:

- Delete old/unused accounts and collected personal information

- o If it's not readily apparent how, you can try these approaches: (1) Go to deletemydata.io/justdeleteme.xyz and find the site there, (2) scroll to the bottom of the page to find the company's privacy policy and look for information on how to delete accounts.
- o Many services will restrict the ability to delete accounts, and especially collected data, to residents of California and/or the EU. You will usually need to fill out a form or send an email - you can try pretending to be a Californian as discussed in the Checkup' "Know your rights..." section.*
- If privacy settings aren't apparent, you may need to review the service's privacy policy. Look for a section with a name like "your rights" or similar. You may need to submit a form, email, or even a letter to opt-out of some collection and sharing. Don't participate in cookie opt-outs.[†]
 - o As with deletions above, many rights, especially the right to request a company not sell your information, will be restricted to California and Nevada residents. Again, you can try pretending to be a Californian (see footnote).

- When reviewing settings:

- o Disable targeted advertising and ad tracking (sometimes called "opt outs")
- o Disable location tracking and history/logging
- o Disable/opt-out of "analytics" or "help us improve your experience" data collection
- o Disable/opt-out of the sale of your information
- o Disable/opt-out of anything that looks or sounds like data collection (look for trigger words: "log," "record,"

"collect," "store," "analyze," and features that "suggest" things for you)

- o Enable two-factor authentication, or additional authentication measures

Checklist: **Services to review for privacy settings** (not comprehensive):

- ☐ Email and other major service providers (see [Google/Gmail](#) and [Microsoft/Outlook.com](#) below, Yahoo Mail, AOL Mail)
 - All Apple and Apple service settings are on-device.
- ☐ Cloud storage providers (i.e. Dropbox)
- ☐ [Amazon](#) (guide below)
- ☐ Car companies (e.g. Ford Sync, Chrysler uConnect)
- ☐ Device manufacturer for any Android devices, especially if you have an account with them (e.g. Samsung)
- ☐ Health/wellness (e.g. MyFitnessPal, Fitbit, Polar, ZocDoc). For fitness apps, also look closely for any public profile/social sharing settings – your data, including location data, is often public by default.
- ☐ Telecommunications companies (e.g. cell phone provider, internet/cable provider)
- ☐ Financial companies (banks, credit cards, where you have loans, PayPal (avoid if you can), CashApp, Venmo, Upromise)
- ☐ Media companies (e.g. Netflix, Hulu, Disney+, Spotify, Pandora)
- ☐ News (e.g. online newspaper accounts, online magazines)

Checklist: **The following are important for submitting do-not-sell requests**– go straight to their privacy policies to find out how to submit a request:

- ☐ Retail sites (Walmart, Target, New Egg, etc)
- ☐ Travel and booking (e.g. TripAdvisor, Booking.com, AirBNB, Expedia)
- ☐ Rewards and loyalty programs (e.g. airline/rental car/hotel rewards programs, grocery store loyalty cards)
- ☐ Anything else

* **A word of caution:** Some web forms may use the words "I attest under penalty of perjury that I am a California resident..." If the form includes those words and you agree, you could actually be committing perjury under California law (if you aren't actually a resident). If it doesn't contain those words, then there is likely no legal risk for pretending to be a Californian (for non-government matters, the law requires those words to be in the agreement). So, do this at your own peril. The odds that any company would take the time to collect proof that you're not a resident and pursue legal action is absurdly low given that no meaningful amount of money is involved, but if you don't want to break the law, then don't "attest under penalty of perjury."

[†] On many websites, you'll see options, especially in privacy policies, to opt-out of targeted advertising based on cookie tracking. **Don't do it.** Ironically, they opt you out of tracking cookies...by placing a tracking cookie on your system. Instead, [secure your browser](#) from these cookies altogether.

Privacy Settings Checklist (back)

The Complete Digital Privacy Checkup – May 2020

GOOGLE ACCOUNT SETTINGS

GOOGLE OVERVIEW

If you own an Android device or use Google services (e.g. Gmail, Google Drive), this process is imperative to your privacy. Google is one of the largest data collection firms, and collects a lot of information on you between devices, services, and its web advertising/analytics surveillance net. This has led many in the privacy community to advocate "de-googling" yourself – finding alternatives for Google services. It's probably a good idea if you're concerned about privacy.

On a desktop/laptop, start by going to:

<https://myaccount.google.com/privacy>

ACTIVITY CONTROLS

From the privacy page, you'll see the option to take the Checkup, which is a good walkthrough, but we're going to take a more granular approach. Under the **Activity Controls** header, select the blue link to "Manage Your Activity Controls."

- ** First, under **Web & App Activity**:
 - o **Uncheck the two boxes** ("include Chrome history..." and "include voice and audio recordings")
 - o **Move the slider to off/paused.**
 - o Click the "manage activity" link, and under the box with a calendar icon, select the blue "choose how long to keep" link. Next, select "Keep for 3 months and then delete automatically."
 - o On the left menu, select "Delete Activity by," then "All time," and confirm.
 - o Return to the overall Manage Your Activity Controls page.
- ** Next, under **Location History**:
 - o **Move the slider to off/paused.**
- ** Next, under **YouTube History**:
 - o **Uncheck the two boxes** ("Include the YouTube videos you watch" and "Include your searches on YouTube")
 - o **Move the slider to off/paused.**
 - o Click the "manage activity" link, and under the box with a calendar icon, select the blue "choose how long to keep" link. Next, select "Keep for 3 months and then delete automatically."

- o On the left menu, select "Delete Activity by," then "All time," and confirm.
- o Return to the overall Manage Your Activity Controls page.
- ** Under **Ad Personalization**, click "go to ad settings" link:
 - o **Turn Ad Personalization off.**
 - o Return to the overall Manage Your Activity Controls page.
- ** Scroll down to the bottom, select the blue **People & Sharing** link next to "to manage contact info from your devices"
 - o **Ensure "Contact Info from your Devices" is off.**
 - o Also recommend you turn off "contact info saved from interactions."
 - o At the bottom of the page, select the blue "Manage Shared Endorsements" link.
 - **Ensure the box at the bottom of the page is unchecked.**
 - o Return to the overall Manage Your Activity Controls page.
- ** Select the blue "your data in the Assistant" link next to "to manage info about installed apps..."
 - o Recommend you turn off all features in this section.

Next, go to: <https://myaccount.google.com/security>

SECURITY SETTINGS

On the security page, you should:

- **Set a new strong password** generated by your password manager (under "Signing into Google").
- **Enable 2-step Verification.** Select the link for 2-step verification and follows steps to set up your authentication token app of choice for 2FA.
- **Review devices logged into your Google Account.** You should revoke access to any old devices or suspicious/unknown devices by going to the "Manage Devices" link and selecting the three vertical dots menu in the top right corner of the device, and then selecting "sign out."
- **Review sites that you have used your Google account to sign into** under "Signing in with Google." As discussed in the checkup, you should either delete the accounts at these sites or create a full account at the site and unlink your Google account. **When you're done with that, ensure there are no accounts linked to Google.**
- **Review linked accounts.** Under "linked accounts," if there are any linked accounts, unlink them.

Google Account Settings (front)

The Complete Digital Privacy Checkup – Privacy Settings Checklist - May 2020

Next, go to: <https://myaccount.google.com/profile>

GOOGLE PROFILE

**** Review your profile and remove any information that isn't required** (name, email, date of birth)

- Ensure profile picture, gender, and date of birth are all "only you" (a lock icon). If not, select and change them.

DOWNLOAD DATA, DELETE A GOOGLE ACCOUNT OR SERVICE

To delete a Google account, Google Service, or download your data from Google, visit: <https://myaccount.google.com/delete-services-or-account>

If you're going to delete your account or a service, you should download the data first. You can also use this process to reduce the information in your Google account (e.g. download all old emails and then delete them from Gmail).

MICROSOFT ACCOUNT SETTINGS

MICROSOFT ACCOUNT OVERVIEW

If you have a personal account for Microsoft services, such as Outlook.com/Hotmail, Skype, Xbox Live, OneDrive, Teams, or Office 365, you have a Microsoft account (not corporate/enterprise accounts though). Many people also log into Windows (especially Windows 10) with a Microsoft Account (formerly a LiveID). LinkedIn accounts are handled separately, unless linked to a Microsoft account. If you don't have one, and are a Windows user at home, it might be a good idea to create one – the data is still being collected, but you don't have any control over it without an account. As you'll soon see, it's a lot of data.

You should also be aware that the below settings are for your Microsoft Account overall, but **Microsoft also segregates service and app-specific settings for each service/app**. So, if you use Skype, you need to go to Skype and review those settings separately, etc.

If you use a Windows device, **you should complete the Windows device settings guide first**, because that is how you control most of this collection.

To get started, go to:

<https://account.microsoft.com/privacy/activity-history>

REVIEW AND DELETE ACTIVITY HISTORY

From this page, you can see *most* of the data Microsoft collects on your activities, and delete it. It's virtually impossible to stop Microsoft's collection completely without leaving the Microsoft world (e.g. switching to Linux), **so your best bet is to visit this page regularly and clear out the data**.

- You will see a complete list of all data Microsoft has collected on your activities (if you don't, select "all data types" on the left menu). Take it in. Google probably had a lot more but they don't make it quite as easy to see this clearly.
- Now, **work your way down each item on the left menu** (Apps and Services, Voice, Search, Browse, Media, Locations)
 - o **** For each one (e.g. Apps and Services), after selecting it, click the red "clear activity" button on to the top right of the list of activity. Then confirm.** Bask in the illusion of power, and then move on.

When you're done clearing all of the collected information, move on to Cortana.

Microsoft Account Settings (front)

The Complete Digital Privacy Checkup – Privacy Settings Checklist - May 2020

Click the **Cortana's Notebook** tab/link at the top of the page (or go to <https://account.microsoft.com/privacy/cortana>)

CORTANA'S NOTEBOOK

Very few people use Cortana, Microsoft's digital assistant, but that doesn't mean it hasn't collected information. From the Cortana's Notebook page:

Click the gray "Clear Cortana Data" button on the right hand of the screen, and confirm.

Next, move on to ad settings by clicking the **Ad Settings** tab/link at the top of the page (or go to <https://account.microsoft.com/privacy/ad-settings>)

AD SETTINGS

From the ad settings page:

- * Toggle off "See ads that interest you"
- * Toggle off "see personalized ads in your browser"

Next, check/manage your security settings by clicking the **Security** tab/link at the top (or go to <https://account.microsoft.com/security/>)

SECURITY

From the security page:

- Select the "password security" box and follow the prompts to **set a new strong password** generated by your password manager.
- Select the "security contact info" box to update/manage account security alerts (you want to receive these in a timely manner).
- **Select the "more security options" box.**
 - o Turn on two-step verification with your authenticator app of choice. If you use Microsoft Authenticator, it can be used to provide login-prompts so you don't have to enter a code.
 - o From this menu you can also optionally set up 1-step logins using Windows Hello or a hardware token ("security key"). Or use Microsoft Authenticator for the same purpose. This isn't recommended.
 - o **You can also delete your Microsoft Account at the bottom of this page, with the link "Close My Account."**

OTHER CHANGES

You can change your account email address at this page: <https://account.microsoft.com/profile/contact-info>

You can edit your Microsoft Account profile here: <https://account.microsoft.com/profile/>

AMAZON ACCOUNT SETTINGS

AMAZON OVERVIEW

The number of adults in the U.S. who don't have an Amazon account can probably be counted on one hand. Amazon collects a lot of data about you, and unfortunately, there's not much you can do about it with their settings options. The company's entire model is built on your data – targeting you with products based on their data stores, and selling cheap devices at or below cost to collect more data to drive more targeted sales. If you have a long history with Amazon, you could consider deleting your account and starting over fresh, just to give them less data, but there aren't good private alternatives for much of Amazon's business (besides devices).

Settings on Amazon's website are also a thick, hard-to-navigate, maze. When you have a spare hour sometime, it's worth it to go deep exploring and see what you find.

First, device and Alexa settings. **If you don't have any Amazon devices (Kindle, FireTV, Fire tablets, Echo/Alexa), you can skip the first two sections and start on the back of this page.**

DEVICE PRIVACY

On a laptop/desktop, go to:

<https://www.amazon.com/hz/mycd/digital-console/deviceprivacycentre/>. If this link doesn't work, you can get here from the Amazon home page (Amazon.com) by clicking the "Hello [Name], Account and Lists" tab (or in that menu's dropdown, the "Your Account" link). Then click the box that says "Your Devices and Content," then the "manage devices," link, then the "Privacy Settings" tab in the white bar at the top, and finally under "Amazon Devices Privacy," click the gray "manage settings" box.

- ** For each listed device, select the device and **untoggle/turn off all switches**. The options vary based on the kind of device, but some common ones are:
 - location-based services, device usage data, interest-based ads, and collect app usage data.
- o For each device that has the "interest-based ads" option, **also click the gray "reset" button below "Reset my advertising ID?"**

When you've completed that, hover your cursor over the "Privacy Settings" tab in the white bar at the top, and select **"Alexa Privacy."** If you can't find it, this address should work:

<https://www.amazon.com/hz/mycd/myx#/home/alexaPrivacy/home>

ALEXA PRIVACY

Either select the box or the left-menu item that says **"Manage Your Alexa Data."**

- * Under **"Automatically Delete Recordings,"** click the **time value on the right with the > symbol** and select **"keep my recordings for 3 months,"** and then the **confirm** button.
- ** Next, toggle off **"use voice recordings to improve Amazon services and to develop new features."**
- * toggle off any toggles available under **"use messages to improve transcriptions."**

Next, on the left-hand menu, select **Review Voice History.**

- Toggle on **"Enable Deletion by Voice"** slider.
- You can review the history of your voice recordings here. To delete them all, change the date range to **"All History,"** and then click the **"Delete all recordings for all history"** link and confirm.

Next, on the left-hand menu, select **Manage Smart Home Devices History.**

- Click the large blue **"Delete Smart Home Devices History"** button and confirm.

Finally, on the left-hand menu, select **Manage Skill Permissions.** Go through the list and review what skills have what permissions and correct as you see fit. Be very skeptical about what a skill really needs to function properly. Some skills are just data-vacuums in disguise.

TURN OFF BROWSING HISTORY

On a laptop/desktop, go to Amazon's homepage at <https://amazon.com>, or from any page on Amazon's site.

On the top right of the page, hover your cursor over "Hello [Name], Account and Lists." Then select the "Your Account" link at the top of the right column. Then, scroll way down to the last part of the white-background part of the page, and next to where it says "Your Browsing History" **select the blue link that says "view or edit your browsing history."**

- In the top right, click "Manage history," and then below that to the left, toggle off **"Turn Browsing History on/off"** and confirm.

Next in the white bar at the top, **select the Your Profile tab.**

YOUR AMAZON PROFILE

Didn't know you had an Amazon profile? Surprise.

- Remove any information in your profile. You can reduce "your public name" to just your first name, or an alias, if you like. When you're done with any changes **click the yellow save button** at the bottom.
- Towards the top of the page, **select "Edit privacy settings" link.**
 - o **Uncheck "Top Contributor Status," and uncheck all boxes under "Public Activity," "Following and badges," and "Lists" headers.** These settings don't change any of the actual lists or activity, it just hides it from your public Amazon profile that anyone can see.
 - o *** Check the "hide all activity on your profile" box.**
 - o *** Check the "hide sensitive activity" box.**
 - o **Ensure the "allow customers to follow you" box towards the bottom is unchecked.**
 - o **Click the yellow save button.**

Next, **return to the main Your Account page** (click "Hello [Name], Account & Lists" box in the top right of the page).

ADVERTISING PREFERENCES

Under the Communication and Content header, **click the Advertising Preferences link.** If you have uBlock Origin turned on, it may give you a warning message here – select the button to allow temporary access.

- **Select the "Do not show me interest-based ads provided by Amazon" radio button, and click save.**

Next, **return to the main Your Account page** (click "Hello [Name], Account & Lists" box in the top right of the page). And then **click the top middle box that says "Login & Security."**

SECURING YOUR ACCOUNT

From the **Login & Security** page, you should:

- Change your email if you're switching to a private email provider.
- **Set a new strong password** generated by your password manager.
- **Turn on 2-step Verification.** Click the "edit" button next to 2-step verification.
 - o **Enable 2-step verification.**
 - o Follow the steps to **add your authenticator app of choice** as your 2FA option. You can optionally add your phone as a backup 2FA option.

DELETE YOUR AMAZON ACCOUNT

Amazon makes deleting an account bit complicated.

If you decide to go this route, here's a how-to guide at WikiHow: <https://www.wikihow.com/Delete-an-Amazon-Account>

SOCIAL MEDIA SETTINGS GUIDE

This guide will walk you through changing your social media settings.

There are walk-throughs for [Facebook](#), [LinkedIn](#), [Instagram](#), [Twitter](#), and [Reddit](#) settings on the following pages.

REVIEWING SOCIAL MEDIA SETTINGS

Social media settings change constantly, so as you work your way through your social media settings, when reviewing social media settings:

- **Be on the lookout for any new options** not mentioned here.
- **It's best just to work your way through every menu**, as settings are often hidden in unexpected places.
- **For most services, the desktop website version offers the most options**, so that's where you should start.

This guide provides walk-throughs for [Facebook](#), [LinkedIn](#), [Instagram](#), [Twitter](#), and [Reddit](#). A * will denote a setting that is critically important to your privacy. **Comb through the menus of any other social media services you use for similar settings** (e.g. Snapchat, Goodreads, Pinterest, etc).

Settings in this guide are based on the desktop website version of each site, both because the web version has the most options and to avoid needing to have multiple guides for each service.

For each social media service:

- ☐ **Double-check privacy settings for social media accounts to restrict public information and sharing.**
- ☐ **Change any old public posts to private (just friends).**
- ☐ **Check profile photos** and replace photos taken in revealing locations with others, or delete and replace with an avatar or non-identifying photo. Please don't use your kids.
- ☐ **Review and delete unnecessary or revealing details** in your social media profiles.
- ☐ **Review your friends and remove suspicious accounts or people you don't know.**
- ☐ **Consider deleting social media apps from your devices and using the website instead** (you can still have the icon on your home screen/app drawer – instructions in right column).

In the following guides, a * denotes a setting that is critically important to your privacy.

MAKE YOUR OWN APP

Social media apps are notorious for devouring as much information about you, your devices, and how you use them as you can.

You can stop this by using the mobile web page version instead. How to do it:

iOS/iPadOS (Safari only):

- Open Safari and go to the service's webpage (e.g. <https://facebook.com>). Log in.
- Tap the Share icon at the bottom (a square with an arrow pointed upward).
- Scroll down to "Add to Home Screen"
- Type the name of the service (e.g. Facebook) above where the web address is.
- Tap "Add" in the top right.

Android OS - Firefox:

- Launch Firefox and go to the service's website (e.g. <https://facebook.com>). Log in.
- Tap the menu icon.
- Tap "Page."
- Tap "Add to Home Screen."

Android OS – Brave:

- Launch Brave and go to the service's website (e.g. <https://facebook.com>). Log in.
- Tap the menu button.
- Tap "add to home screen."

DON'T LINK ANYTHING TO SOCIAL MEDIA

Lots of apps and websites want you to link your social media account to them. Don't. They want this because it's a way to better track and get more information about you.

(front)