Be Location Safe

ObscureIQ

To get location safe, stop leaking your location and cleanup the data you have already spilled.

Threat Level	Stop Leaking Location Data	Delete Past Location History
Low	**Disable Specific App Tracking** Stops specific apps from tracking you. Blocks invasive apps, esp. large platforms: Facebook, Insta, Messenger, TikTok, YT, GMaps, Uber, Amazon, LinkedIn, X/Twitter, Snapchat.	**Auto Delete after X Days** You can also choose to automatically delete your location history after a certain period of time: 3 Months, 18 Months, or 36 Months. **Instructions**. link
Med	**Disable Global Ad Tracking** Stops majority of location data leakage. Removes the ability of AdTech to track you and share your info via your Mobile Ad ID (MAID). link **Instructions**.	**Delete All Google Map Data** Delete your loc history stored by Google Maps. Maps holds tons of location history. Other suspects include: social media, weather, & fitness tracking apps. link **Instructions**.
Med	**Enable Airplane Mode** Quick toggle to disable your phone's ability to share its location. GPS is still enabled, but cellular, Bluetooth, and Wi-Fi are off, preventing communication of location. [Your phone is mostly incommunicado in this state.]	**Delete All Location History** Delete your location history stored by the Google/Apple ecosystems. Note that it will likely be in more than one location.. link **Instructions**.

To truly be Location Safe, you need to go farther.

High	**Disable Location Services** Disabling Location Services effectively halts most forms of location tracking. It turns off your GPS. [Apps like Maps will not work.] Even with Location Services turned off, your phone is susceptible to tracking. This can happen via cell towers, public Wi-Fi, cell site simulators (stingrays), Bluetooth, IP addresses, and malware. You are pretty safe with Loc Services off, unless you are being targeted by law enforcement, governments, or bad actors.	**Wipe Location History from Data Brokers** Deleting your location history from your phone does NOT delete it from the 400+ location brokers who have collected it and are selling it. You will need to submit requests to each for removal. The only viable alternative we know of is an **Obscure Footprint Wipe**. link Unlike other data deletion services, it purges location history.

High Threat Level Actions give you the best Location Protection, but nothing is 100%.
Determined actors can still find you. Here are additional steps you can take:

High	**Defeat Web-based Tracking** When surfing the web, your location can be exposed via IP-based location tracking. Browser fingerprinting and cross-site tracking can also occur. To mitigate this tracking: -- Use **a good VPN** (not a free VPN) link -- Use **a Privacy-focused Browser** link -- Use **a privacy-focused Search Engine** link	**Delete Your Current Address From Data Brokers** Delete your personal info from people search engines. This is usually done as part of a digital footprint wipe of your personal data from data brokers. However, the effort can be more targeted. Current address deletion is tricky. Be sure to consult an org like **ObscureIQ** to understand what's possible. link
High	**Avoid Malware Tracking** To cut the risk of malware being used to track you: -- Don't install extra apps. Every new app is a risk. Remove unfamiliar apps. If you don't know what it does, delete it. -- Install updates regularly to your OS, Browser, apps -- Scan regularly for spyware and malware -- Protect your critical accounts (email, banking, healthcare) with **strong passwords** and two-factor authentication. link	**Install a GPS Spoofing App** Be careful the app isn't malware! -- Install a specialized app (**GPS Spoofer**) that lets you fake your location, sending it instead of your true location to other apps in your phone. link -- Be sure to change your spoofed location often.
High	**Avoid Social Media Location Harvesting** To keep Social Media apps from tracking you: -- Turn off location tracking on your social media app -- Disable **location tracking on your phone's camera and remove photo EXIF metadata** link -- Avoid posting **photos that reveal geographic clues** link (signposts, skylines, flora, named buildings, etc.) -- Avoid posting text that reveals your location. "Heading to the gym." "Going to Cancun for vacation." "Just saw Joe in DC." "Beautiful morning in West Palm Beach."	**Photo Tracking** To help keep your photos from revealing your location: -- **Scan social media accounts** and remove photos that can reveal location history, patterns. link -- Remove posts containing text that reveals your location. "Heading to the gym." "Going to Cancun for vacation." "Just saw Joe in DC." "Beautiful morning in West Palm Beach."
High	**Configure/Disable Assistants, IoT Devices** Google Assistant, Amazon Alexa, Apple Siri, and emerging AI assistants like ChatGPT and Gemini utilize your location data to tailor and enhance their services.. IoT devices like smart watches, smart TVs, and smart thermostats often reveal your location, even if it's just at and around your home.	**Wipe Your Assistants and IoT Devices** Depends on the assistant or device.
High	**Lock Your SIM Card** SIM swapping is a type of fraud where the attacker tricks your mobile service provider into transferring your phone number to a new SIM card. Once the attacker has control of your phone number, they can use it to track your location. A locked SIM card is much more difficult to attack. **Instructions**. link	
High	**Vehicles Leak Your Location...** Nearly every new car contains GPS and other tracking mechs. It will automatically share your data and location. Vehicles registered to you are tracked when you drive them. Automated License Plate Readers (ALPR) are all over now. Vigilant has installed over 15K and Flock has installed over 6K. Many police cars contain mobile readers and toll roads contain specialized readers. As tech improves and proliferates: * Some ALPR cameras can recognize your face if processing is applied. * Traditional CCTV cameras feeds can harvest ALPR data.	**Wipe Your Vehicle Data** Wipe your personal data from any cars you own before selling them. Wipe your personal data from any rental cars after usage. Connecting your phone to a rental car is a bad idea - it sucks up your data. link For more info see **Privacy4Cars**.
High	**Your Face Leaks Your Location...** With the widespread adoption of facial recog, your face can inadvertently reveal your whereabouts in various public spaces across the USA. Surveillance cameras are becoming increasingly prevalent, particularly in high-traffic areas, transportation hubs, and border crossings.. ALPRs now feature facial recog, while CCTV feeds are mined for facial data.	**Avoid Facial Recognition** Low-tech: Know where cameras are and avoid scanning. Obscure face with hats, sunglasses. High-tech: Use anti-facial recognition clothing and/or makeup. Glasses with infrared lights can confuse some systems.