



SILICA

WHO KNOWS WHERE YOU ARE

You carry a beacon and call it a phone. Most of what it tells, it tells quietly, to more people than you think. None of this needs fear. It needs ten minutes and a few switches.

◆ Your photos carry a map

Phones write the GPS position into every photo they take, as hidden data in the file. Big social apps usually strip it on upload. Texts, email, AirDrop, cloud links and "send as file" often keep it, so the person who gets the photo can see where it was taken, sometimes down to your front door.

- **iPhone:** in the share sheet tap Options and turn off Location. To stop tagging altogether: Settings > Privacy & Security > Location Services > Camera > Never.
- **Android:** open your camera app's settings and turn off the location or geotag option.

◆ Apps that know too much

Many apps ask for location once and keep it forever. Few need "Always", and fewer need your exact spot. A weather app works fine knowing only your town.

- **iPhone:** Settings > Privacy & Security > Location Services. Per app choose Never or While Using, and turn off Precise Location where it isn't needed.
- **Android:** Settings > Location > App location permissions. Pick Allow only while using and turn off Use precise location.

◆ Your phone keeps a diary

Both phones can record the places you go and how long you stay. Useful to you, and to anyone who gets into your phone or account.

- **iPhone:** Location Services > System Services > Significant Locations. Review, clear, or turn off.
- **Google:** in Google Maps tap your profile picture > Your Timeline. Turn it off or set auto-delete.

◆ Who you are sharing with, right now

Live location sharing is easy to start and easy to forget. An ex, an old friend, a shared family plan or a car app may still see you.

- **iPhone:** Settings > Privacy & Security > Safety Check shows everyone you share with and can stop it all at once. Also the People tab in Find My.
- **Google Maps:** profile picture > Location sharing.
- **Snapchat:** on the Map, tap the settings gear and turn on Ghost Mode. Check WhatsApp live location and Instagram's map in your messages too.

◆ Trackers that ride along

Coin-sized Bluetooth trackers (AirTag, Tile, SmartTag and others) are made to find lost keys. Slipped into a bag, a coat or a car, they find people. Phones now warn you when an unknown tracker travels with you, across brands, but only if the warning is on.

- **iPhone:** keep Bluetooth, Location Services and Find My notifications on. You'll get an alert like "AirTag Found Moving With You". Tap it to make the tracker play a sound and see how long it has been near you.
- **Android:** Settings > Safety & emergency > Unknown tracker alerts (on some phones under Settings > Google). Keep alerts on, and use Scan now any time you're unsure.
- Check where these hide: bag linings, coat pockets, under car seats, in the boot or wheel arches.
- If you find one and feel unsafe, think before you destroy it. It may be evidence, and the owner may notice it went quiet. Reach out to local police or a domestic violence service first.

◆ Your accounts are a back door

Anyone who knows your Apple or Google password, or has your phone unlocked for a minute, can often see your location from their own device. No tracker needed.

- Review signed-in devices: on iPhone, Settings > your name and scroll down. For Google, myaccount.google.com > Security > Your devices.
- Change passwords someone else may know, and turn on two-step verification.
- Unfamiliar apps, a battery that drains fast, or settings you didn't change can be signs of stalkerware.

◆ What every website sees

Every site you visit sees your IP address. That usually reveals your rough city or region, not your home. It is how ads seem to know your town. A trustworthy VPN hides it from websites, though the VPN company can then see it instead.

This page asked your permission for your exact spot. Most of the web never asks.

◆ Your address is probably for sale

Data brokers and "people search" sites stitch together public records, old sign-ups and purchase data into profiles with home addresses, relatives and phone numbers. Search your own name and town to see what comes up. Most sites have an opt-out form, usually buried at the bottom of the page, and paid services can file the requests for you. In some places, such as the EU, the UK and California, the law gives you the right to demand deletion.

◆ If you think someone is watching

- Make changes from a device the other person has never had access to. Stopping a share or removing a tracker can be noticed, so if that could make you less safe, talk to a support service first.
- The Coalition Against Stalkerware, stopstalkerware.org, and the EFF's Surveillance Self-Defense, ssd.eff.org, have step-by-step help.
- If you are in danger, call your local emergency number.