A Guide To Device Tracking: Smartphones

https://www.reddit.com/r/runaway/comments/mahc2c/a_guide_to_device_tracking_smartphones/

Introduction

Welcome to this guide on smartphone tracking and how to safely use your Android or iPhone without unintentionally revealing your location and sensitive information. This guide will go over the most common ways your location and private information is compromised and how to protect your most sensitive data from the authorities and big tech companies.

You may wonder why you need to protect yourself from big tech companies, like Amazon, Apple, Google, Facebook, Microsoft, etc. The reason is, these companies collect a ton of personal data about you. They track and keep a permanent record of your search history, every private message you've sent, every link you've clicked, everything you've liked, every website you've visited, your email inbox, your location history and much much more. All this data is also available to the authorities, as they can by law order any companies who's services you use to hand over all the data they have on you. Therefor it's important to prevent these companies from obtaining your sensitive data in the first place. Almost their entire business model relies on selling your personal data, so naturally they take big steps to gather as much of it as possible. There's a reason most of the services these companies provide are free. You don't pay with your money, you pay with your data.

This guide will not make you anonymous or completely secure from all types of tracking and data collection, as that's very difficult and beyond the scope of this guide. The aim of enhancing your security and privacy is to exhaust the resources of your adversaries, to the point where they run out of resources or simply give up. This guide is intended to be a basic tutorial on how to protect your most sensitive data and prevent the most invasive forms of tracking and data collection, whilst being beginner friendly, easy to understand, not impacting usability or convenience too much and not requiring advanced technical knowledge. So without further to do, let's get started.

SIM Card & IMEI Number

Your Subscriber identity module (SIM) card is by far the most common and easiest way the authorities are able to track you down. Your SIM Card contains your unique phone number, among other things, and your phone number is obviously directly associated with yourself. As you move around, you phone automatically connects to cellphone towers so you can send and receive calls and SMS texts and use mobile data. However your cellphone carrier can actually pinpoint your phones near-exact location as it connects to these cellphone towers and use this to track you, via cellular triangulation. This information is also obviously shared with the authorities upon request.

A common myth to avoid being tracked is to simply remove your SIM card. This will however not help. Your phone also has something called an International Mobile Equipment Identity (IMEI) number. This number is a unique number that is physically attached to your phone. This number is automatically sent any time your phone connects to any cellphone tower. Anyone who knows this number belongs to your phone will be able to track it. Changing it is complicated, technical and requires special equipment. Changing or even just possessing the tools to change it is even illegal in some countries.

What this means is that whilst you can change your SIM card, your IMEI number stays the same. Even if you were to insert a brand new SIM card into your phone, then the IMEI number would still be the same and the cellphone carrier would see that it's still the same actual phone as before. This is a problem because as you might know, you can still actually call emergency services when you don't have a SIM card inserted. That's because even without a SIM Card, your phone is still connecting to cellphone towers, and thus still broadcasting your unique IMEI number, allowing you to still be tracked via cellular triangulation, as discussed above.

So how do you solve this problem? You need a new phone with a new IMEI number that's not associated with you and cannot be tied back to you in any way, or prevent your phone from being able to connect to cellphone towers. The latter is actually fairly easy, just turn on airplane mode. Airplane mode disables the functionality in your phone that enables it to connect to cellphone towers. However the drawback of this is obviously that you wont be able to send and receive calls, texts and use mobile data. This will limit you to using Wi-Fi networks only. You must also remember to keep airplane mode on all the time. The second it goes off, your phone will connect to the nearest cellphone tower and broadcast it's IMEI number again.

If you don't want to be limited to using Wi-Fi networks only, then you need a new IMEI number and SIM card. As mentioned previously, changing the IMEI number on your current phone is just not practical for the vast majority of people. Thus the only other option is to obtain a new phone that of course has a different IMEI number. However you must be careful when purchasing this new phone. If anyone is able to link you to the new phone, then that phone would of course be compromised and you'd have to get a new one. To acquire an anonymous phone you must:

- Purchase it using cash (to avoid the bank knowing about it)
- Purchase it somewhere where you wont be recognized
- Have no other phones or traceable devices on your person
- Not take it with home or to any place associated with you (unless powered off or Airplane mode is activated)
- Never have your new phone in close proximity to your old phone (unless powered off or Airplane mode is activated)
- Make sure no one knows about it

I recommend ditching your old phone and getting a new one only after you've run away and gotten out of town. If you do this and apply some healthy common sense, you should have an anonymous phone that is not associated with you in any way.

Now you'll want a SIM card so you can call, send SMS messages and use mobile data and this is unfortunately where you might be screwed. Most countries in the world require valid ID to purchase/activate a SIM card. This is obviously a disaster if you want to avoid your new phone being associated with you and not be tracked. Go to https://datawrapper.dwcdn.net/9H6HA/6/ for a map of which countries require ID to purchase and activate a SIM card. (Note: Sweden now also requires mandatory SIM card registration)

If you're in one of the red countries, you are sadly out of luck and will have to use your phone as a Wi-Fi only device, like discussed above. However if you are within one of the green countries you are good and may acquire a SIM card following the same steps as you did purchasing the phone. It's recommend to buy a pre-paid SIM card, as they don't require you to sign up to any payment plan, which of course would require a bank account and compromise privacy. Pre-paid SIM cards are a simple one time purchase, no extra strings attached.

IP Address

An IP address is a unique identification number assigned to any Wi-Fi router you connect to. It’s required for basic internet functionality, but it can also be used to reveal your location. Normally your IP address only reveals your approximate location within a pretty large area, but even that is enough for authorities to track your movements and locate you. They can even request the local Internet Service Provider (ISP) to provide them the exact location of the WiFi router you connected to. When accessing websites, online accounts and generally anything to do with the internet, the sites you visit know your IP Address and many log it. Authorities can request the site to hand over any IP Addresses that have connected to their site. So if for example you have logged into your Reddit account, and the authorities know that account belongs to you. They can ask Reddit to hand over the IP Address that you used to log into your account and locate you from there.

The simplest way to prevent this is using a Virtual Private Network (VPN). A VPN will hide your IP Address from any site you visit and hide your internet traffic from your ISP, thus concealing your real world location.

Remember a VPN does not make you anonymous at all, this is false marketing. You are simply using their IP Address to connect to the internet, which means they have access to your real IP Address and can actually monitor and log your web traffic if they wish. Authorities can also contact them and demand them to disclose your real IP Address and web traffic. That’s why it’s extremely important to pick a secure and trusted VPN Provider with a good track record and privacy policy. Unfortunately, there are very few that actually are trustworthy. Even popular paid VPNs like NordVPN and Surfshark have numerous issues and aren't to be relied upon if you wish to increase your privacy. Luckly there are a few out there that really do care about your privacy and can back it up with good track records and proper security audits. They are the following:

- ProtonVPN – Offers a free plan with unlimited data and servers in the US, Netherlands and Japan. No details required to sign up, except email.
- Mullvad – Costs $5 USD per month, accepts cash and requires no details to sign up.
- IVPN – Costs $6 USD per month, accepts cash and requires no details to sign up.

Location Services

Many apps, like Snapchat, Google Maps, Facebook, Messenger, Instagram, TikTok, and more track your location via GPS, store your location history indefinitely and will happily sell it to whoever wants to buy it. If anyone was to gain access to these accounts, or the companies were forced by the authorities to reveal your data, then obviously you would be found very quickly.

To prevent these apps from tracking you, preferably just delete them, or disable their ability to access your location.

- For iPhone go into "Settings > Location Services" and select each app and set them to Never
- For Android go into "Settings > Apps and Notifications > Permission Manager > Location" and select each app and set them to Deny

You should also straight up disable Location Services all together when your not using it. Disabling Location Services also has the neat benefit of increasing your battery life.

If you need to use a digital map like Google Maps or Apple Maps, firstly try asking around for directions instead if you can. If you absolutely need to use a digital map with GPS, then temporarily re-enable Location Services (make sure you’ve blocked location access to other apps, like discussed above) and use a more privacy respecting map service like Organic Maps. You don’t need an account to use it, it's completely free, works offline and a great alternative to the more privacy invasive Google and Apple Maps. If for whatever reason you still need to use these maps, don’t install the apps, use them in your web browser instead, without logging in to any accounts.

Email Address

Your email address is one of your most valuable and at the same time vulnerable things you have. It is the single point in which all your online accounts are tied to, you may also use it for communication. If your email address was to be compromised, everything tied to it would be too. That’s why it’s very important to properly secure your email and use an email provider that can be trusted to keep your emails safe.

You are probably currently using Gmail, Outlook, Yahoo, AOL or something similar as your current email provider. All these email providers are owned by big tech companies that sell your data. They don't encrypt your email, so they are able to access your entire inbox, which they actually do in order to sell and serve you ads. This among many other reasons is why these companies cannot be trusted with your personal information.

To prevent this, you should switch to an email service provider that respects your privacy, doesn’t read or log your emails, and most importantly, encrypts you emails properly so no one else can read them, not even the email service provider themselves. So if authorities were to request they hand over your emails, then they would be unreadable. Currently there are two popular options with very good free plans that fit the bill. ProtonMail and Tutanota. Both of them respect your privacy and have excellent track records. It’s highly recommended you use one of the two here, instead of the one you're currently using now.

Social Media

Your social media contains a lot of information about you. It is usually one of the first things people try to access. It could contain sensitive conversations, forum posts, personal information, friends, plans, and much more. Your social media accounts are likely all tied to your real identity in some way. Even the ones you're sure no one knows about. The last thing you want is someone discovering an account you forgot to log out off, or your friends disclosing an account belongs to you, when you didn’t want them to.

Your best bet is to simply just delete all your social media accounts. They likely contain a ton of information about you, their apps are full of trackers, and simply changing the password wont prevent the authorities from obtaining details saved on your accounts.

If you wish to continue using social media. You should create new accounts, with new usernames, passwords, 2 Factor Authentication, one of the above mentioned emails and without using any of your real information (you can write fake info for most account signups that request your real info). Create them whilst using a VPN, so the accounts can't be linked to your current location and possibly you. Be careful what you share on those accounts and only share your new accounts with people you trust or people who don’t know who you really are.

Additionally make sure to go through all your accounts privacy settings and disable as many permissions as possible.

Communication

You may wish to have a line of communication back to your family or friends. Therefor picking the right way to communicate as to not accidentally reveal your location is crucial.

It’s recommended not to use social media, like Instagram, Discord, etc, as your primary form of communication, as most of them don’t use encryption and have terrible privacy policies. The companies themselves can easily monitor and gain access to your “private” conversations, and subsequently the authorities.

Sending messages using SMS (the green bubbles) is also insecure, authorities can easily intercept your messages and cellular towers can (and do) save and see the contents of your messages. Phone calls are in a similar boat.

It’s heavily advised you switch over to an end-to-end encrypted messaging app like Signal or Session as your primary communication platform. You should ditch other messaging apps like WhatsApp, Telegram, Allo, Facebook Messenger, etc. These ones are simply insecure. Many of them don't encrypt your messages by default and the ones that do use weak encryption and can still access plenty of identifiable information and in some cases can even bypass the encryption all together. They’re all rather dubious and collect a lot of you data no matter what you do and don’t really care about your privacy at all. Signal and Session on the other hand do respect your privacy, have great track records (unlike the other apps), are completely free and use proper encryption that actually stops 3rd parties from being able to read your messages and access other identifiable information.

Keep in mind the person on the other end must also use Signal or Session respectively. Signal also requires a phone number to sign up with. Session on the other hand does not require a phone number to use, but currently calls are in beta, so you and the recipient will both have to enable it in the settings to be able to call each other.

Remember, no matter how secure your way of communication is, there is nothing stopping the person on the other end from revealing your messages to others, screenshotting conversations and recording calls. So use caution whenever you communicate with someone and don’t share any sensitive information unless you absolutely need to and can 100% trust that person.

Exif Data

Exif data is hidden metadata attached to photos and videos. This data can easily be viewed by the right programs. Most Exif data is harmless, however it can contain the time/date and geographical location the photo or video was taken and thumbnails (unedited version of your photo). This is why you should make sure to remove your Exif data from your photos and videos before sharing them.

To avoid having your media tagged with the geolocation they were taken, stop your camera app from accessing your location, as discussed in the Location Services section above.

Many of the biggest media sharing platforms also automatically strip identifying Exif data from what you share, but it's likely they log that removed data. So it’s recommended you remove it yourself, and not rely on the site you're uploading to. You can remove Exif data yourself with Exif Eraser on Android or Metapho on iPhone. Also bonus, Signal and Session automatically removes the Exif data on any photos and videos you send!

Keep in mind Exif Eraser and Metapho can only remove the Exif data from photos. Currently there aren't any good, trusted tools to remove Exif data from videos on mobile. So if you wish remove Exif data from videos, you’ll have to do so on a computer. Or you could send a video through Signal or Session to yourself and then re-download the exif cleaned version.

Final Steps

Don’t use Google Chrome as your internet browser. It's terrible for privacy and logs all of your activity, it's essentially spyware. Using Google, Bing or Yahoo as your search engine is also not advised, as they also log your entire search history and store it indefinitely.

For iPhones, Safari is a perfectly fine browser to use. However there are a few tweaks to be made to it.

- First you should go into "Settings > Safari > Privacy and Security" and enable Prevent Cross-Site Tracking. This will strengthen Safari's ability to prevent trackers, without impacting usability.

- You also want to change your default search engine to something that won't log your activity. To do this go to "Settings > Safari > Search > Search Engine" and select DuckDuckGo as your search engine.

- You should also enable Private Browsing. To do this open Safari and tap the Tabs button, located in the bottom right. Then, expand the Tab Groups list and select Private. This offers quite a few additionally privacy benefits you'll want. However keep in mind that whenever you close Safari, all cookie and site data will be deleted, so you won't stay logged into accounts even if you click Remember Me.

- Lastly I recommend installing the AdGuard extension. This will not only block ads, but also offers some additional privacy benefits when surfing the web.

For Andorid I recommend Brave as your browser. This browser has a built in search engine, Brave Search (you can switch to DuckDuckGo if you prefer that), and automatically blocks both ads and trackers. Like with Safari for iPhones, we can make a few tweaks here as well to improve the effectiveness of Brave. In the Brave browser, go to Settings > Brave Shields & privacy.

- Under "Brave shields global defaults" go into "Block trackers & ads" and select Aggresive

- Under "Clear browsing data" select Clear data on exit (Keep in mind that whenever you close Brave, all cookie and site data will be deleted, so you won't stay logged into accounts even if you click Remember Me.)

- Under "Social Media Blocking" uncheck all components

- *Under "Other privacy settings" go into "WebRTC IP handling policy" and select Disable Non-Proxied UDP. After that you'll want to uncheck the following: IPFS Gateway, Allow privacy-preserving product analytics (P3A), Automatically send daily usage ping to Brave, and Automatically send diagnostic reports and if it's not too inconvenient you should also select Close tabs on exit*

It's recommended you secure all your accounts with 2 Factor Authentication (2FA) if available using a 2FA app like Aegis Authenticatior for Android or Ravio OTP for iPhone, and strong passwords, preferably using a password manager. Be careful, many popular password managers out there can't be completely trusted and aren't safe to use, like 1Password and Lastpass. It's highly recommended you use BitWarden, a secure, cloud based password manager that's very convenient with an excellent track record that syncs your passwords across devices. Or KeePassDX on Android, a more secure, though less convenient option.

It's also good practice to disable Bluetooth, AirPlay, Mobile Hotspot, Mobile Data and Wi-Fi when not in use.

If you've got a computer or any other devices that your leaving behind, make sure to erase all the data on them. Passwords can easily be bypassed with physical access to a device.

Conclusion

- Acquire a burner phone or keep airplane mode enabled at all times

- Disable access to Location Services for as many apps as possible

- Use one of the recommended VPNs
- Switch your email provider to either ProtonMail or Tutanota
- Use Signal or Session for communication
- Use Exif Eraser or Metapho if you are going to be sending photos
- Delete your social media accounts
- Disable as many permission as possible in your phone and accounts privacy settings
- Use BitWarden Password Manager or KeePassDX
- Use 2 Factor Authentication where available
- Use the Brave browser or Safari and tweak their settings
- Disable Bluetooth, AirPlay, and Mobile Hotspot when not in use
- Erase all data on any devices left behind

Note we've only gone over smartphones in this guide, whilst some of this applies to computers as well, your computer is probably insecure and is still monitoring most of what you do on there, unless you're using a reputable Linux distribution

With all of these steps and a good amount of common sense, anyone trying to track you using your phone or internet usage will have a significantly harder time doing so and will need to spend much more effort and resources. There are a ton more things you can do to increase your privacy and security and I highly encourage you go out and do your own research.