UBINODES

Research:
GPS Tracking

Research: GPS Tracking.

Your cell phone provider can access your GPS location at any time, even when you have turned off location services, putting your privacy at risk.

1. This is an informational guide for:

- How GPS works on your mobile device.
- What your cell phone provider does without permission.
- How your SIM card can be used to spy on your location.
- Finding out whether you can stop state-sponsored criminals from locating you through your mobile device.

2. Reviewing SIM backdoors and location security:

1. Your mobile carrier has access to your GPS location at any time.
2. State-sponsored criminals could locate you through your mobile device without permission.
3. Locking your phone or turning off location services will not prevent your location from being found.
4. Apple states in its privacy terms that "your iPhone's location information may be used when you place an emergency call to aid response efforts regardless of whether you enable Location Services."
5. Any phone, even phones without SIM cards, can make emergency calls.
6. If emergency services can locate you when you make a call in any circumstance, even a phone without a SIM can be traced using geo-location.

3. How your GPS is used on your mobile device:

1. Users of iOS or Apple mobile devices have the ability to turn off Location Services for anything but emergency calls.
2. Android users are given a choice of High Accuracy, Power Saving, or GPS only and do allow you to select which apps use GPS, but do not give you the choice to turn off Location Services.
3. Your phone's location is triangulated every 10 seconds to access the closest cell tower, making it easy for emergency services to find you.
4. If it is so simple for emergency services to find you, there is nothing stopping state-sponsored criminals from doing the same.
5. Removing your SIM will not change the ability for your phone to be traced since the trace is based on the connection to the cell tower.
6. If spyware is installed on your device, your location could be shared with criminals and hackers.
7. Spyware can steal more than your location, but also can take control of your mobile device's camera, contacts, text messages, and eavesdrop on conversations you are having.

4. Why tracing you without permission is wrong:

- Emergency services might be able to use it to locate you in an emergency, but cannot always get a precise location.
- If emergency responders cannot effectively use the location option on a phone, it serves no real purpose.
- You should be able to choose whether your provider can access your location as it is a privacy concern.
- State-sponsored criminals could use your location as incriminating evidence to attempt to prove you were somewhere.
- Since the trace is not accurate enough to pinpoint where someone is exactly, the data that state-sponsored criminals could use against you would be inaccurate.
- The inaccurate information could still be pressed as fact, even when it isn't.
- Your whereabouts should not be information that others have access to.
- Tracking people is the equivalent of Orwell's "Big Brother."
- Software like Wireshark can use SS7 and OpenstreetMap to locate users on the network and pinpoint coordinates. This skirts the line between legal and illegal, making it difficult to prosecute abusers of the software.

5. How can you protect your location privacy:

- Do not use geo-location on the internet if it has asked for your permission.
- Make sure location services are as locked down as your phone will allow. This may be impossible depending on your specific device an operating system.
- Ensure that your device's ability to store your location history is also turned off. If you find that your phone is saving your location data, you should clear any history.
- Block your location data by going into your browser's settings and adding a Do Not Track (DNT) HTTP header.
- DNT's are recognized by most browsers, but not by all websites. The browser cannot control whether a webpage honors a DNT request.
- Use encrypted networks whenever possible.
- Make sure that your cookies are turned off on your browsers for any mobile device you use. This is in the browser's settings.
- Cookies are used by marketing teams to track your internet habits to market better to you.
- The same tracking information could be utilized by state-sponsored criminals. Keep cookies off.
- Download anti-tracking apps on your mobile device.
- Anti-tracking apps and anti-tracking software scan your device to see if it is being spied on.
- Do not use Google. It is hard because Google is everywhere and all of us use it for something. But Google Tracking can easily find and store your location.
- To stop Google from knowing your location, you can use apps or add-ons like Location Guard to stop it.

- Make sure the Web Real Time Configuration (RTC) is turned off. If it is on, servers could request information about your device, making it easy to trace your location.
- Get a VPN for mobile security. Just like on a computer, a Virtual Private Network (VPN) encrypts the data going from your device, meaning the IP address is completely hidden. You could use Protonmail VPN : https://protonvpn.com/

6. Conclusion:

All mobile devices have the ability to track your location, even though the tracking ability is not always accurate. Since the location services are advertised as being helpful in an emergency and are proven to not be exact or accurate, there is no justification for your location to be found by anyone, including emergency responders.

If an emergency responder has access to a general location for you, state-sponsored criminals also have the ability to trace your location. It is impossible to simply turn off Location Services on your mobile device to really stop the ability to track you. The safest thing to do is to turn off Location Services on your mobile device as much as they will allow you. Then, you should install a mobile VPN, like Le VPN, in order to encrypt your location so it cannot be seen or used by anyone, including state-sponsored criminals.

Because a phone has to access a cell tower in order to operate at all, your location is being detected any time it is used. Whether the cell tower will know what phone it is looking at will depend on whether you are able to use a VPN to encrypt the signal.

