HOW THE POLICE CAN DETERMINE YOUR LOCATION, AND HOW YOU CAN BETTER CONTROL ACCESS TO YOUR LOCATION DATA

Where is my phone's location data stored?

Your phone can be located in two main ways, using GPS or mobile network location:

1. GPS

- GPS (that stands for Global Positioning System) uses satellite navigation to locate your phone fairly precisely (within a few metres), and relies on a GPS chip inside your handset.
- Depending on the phone you use, your GPS location data might be stored locally and/or on a cloud service like Google Cloud or iCloud. It might also be collected by any app that you use that has access to your GPS location.

2. Mobile network location

- Mobile network location (or Global System for Mobile Communications (GSM) localisation) relies on your cellular network, and can be determined as soon as you are connected to the network (i.e. your phone is switched on and not in airplane mode) but is far less precise than GPS. Your approximate location can be determined with an accuracy range of a few dozen metres in a city, or hundreds of metres in rural areas.
- This location data is stored by your network provider.

Other methods can also be used to determine your location indirectly, such as open wifi access points and Bluetooth beacons your phones connects to or location metadata embedded in your photos.

How can my location data be accessed?

There are a number of methods the police can use to can gain access to your (phone) location:

1. GPS

- Accessing GPS location data depends on where the data is stored. It can be done using a 'mobile phone extraction' device, which plugs into your phone and downloads all the data stored on it, including details of locations you have visited.
- Access to your GPS data may also be possible through device hacking, an advanced technique which might not necessarily require physical access to your phone and could be done remotely.
- If your GPS data is also stored on an online account (e.g. iCloud or Google Maps), it can be accessed through cloud extraction technologies or legal requests to the companies that store that data.

2. Mobile network location

- Your approximate location data can be accessed by the police through your service provider.
- This means that the police don't need access to your phone handset to determine that you were within a certain proximity of a protest.
- Another means of accessing this same information is to use an 'IMSI catcher' (also known as a 'Stingray'), a device deployed to intercept and track all mobile phones switched on and connected to a mobile network in a specific area.

How to better control your location data

1. GPS

- The best way to prevent your location being accessed is to limit the generation of the location data in the first place.
- In the case of GPS, it can be as simple as switching off your GPS (often referred to as 'location services'). But bear in mind that the location data of any previous occasions where you did have it switched on might still be accessible.
- If you still need to use GPS on your phone, check individual apps' permissions to access your location to minimise the spread of this information.
- Removing permissions to access your location for all apps can prevent this data being stored on an online account.
- If you absolutely need an app to have access to your GPS data, inspect the settings of that app to ensure that you understand if your location is being stored online or just locally on your app. For example, if you use Google Maps while logged into a Google account, you might want to disable location history in the settings so that your location history won't be stored in your Google account.
- If you've taken pictures with your location services switched on, the location where the picture was taken might be included in the metadata (known as EXIF data) of the image. You might want to disable location services while taking pictures, or you can use software or an app to erase this EXIF data afterwards (for example, the Signal messaging app erases EXIF data when you send images).
- Similarly, turning off your wifi or Bluetooth can prevent your phone from connecting to unwanted access points and providing indirect location information.

2. Mobile network location

- When it comes to mobile network location, the only way to have control over it is to prevent connection to the network at all.
- Having your phone switched off, in airplane mode, or in a faraday cage will prevent connection to your mobile network, and therefore make GSM geolocation impossible. A faraday cage or switching off your phone prevents any and all types of connection to any phone network. Whereas just using airplane mode means that some types of connections can still be made (e.g. Bluetooth or GPS).

