HOW THE POLICE CAN ACCESS YOUR PHONE'S 'UNIQUE IDENTIFIERS', AND HOW YOU CAN TRY TO MAINTAIN YOUR ANONYMITY

What are my 'unique identifiers' and where are they stored?

- Your phone and your SIM card contain unique identifiers about you, which can be accessed by the police to identify you.
- The IMSI (International Mobile Subscriber Identity) is a unique number associated with your SIM card. It doesn't change, even if you put the SIM card into a different phone.
- If you have a mobile phone subscription, the IMSI will be associated with personal information such as your name and address.
- The IMEI (International Mobile Equipment Identity) is a unique number identifying your phone (the device). So if you change your phone, you will have a new IMEI.
- IMSI and IMEI cannot be altered otherwise, and they can be linked to information about you (e.g. name, address) or your device (e.g. brand, model).
- Ad ID: Ad Identifiers are different from IMSI and IMEI in that they can change over time. Ad IDs are used by advertisers in apps and websites to uniquely identify you online and offer services such as targeted advertising. Ad IDs are not directly linked to your personal information (e.g. your name) but can be associated with other revealing data about you (e.g. geolocation, apps used, websites visited etc). The Ad ID is generated by your phone's operating system, and is usually visible in the settings of your phone. It can be manually renewed.
- Other identifiers: There are a few other components in your phone with unique identifiers, such as the MAC address for your wifi antenna, or the BD_ADDR for your Bluetooth module.

How can my unique identifiers be accessed by the police?

- Your IMSI and IMEI can be obtained by the police with an 'IMSI catcher', a device deployed to track all mobile phones switched on and connected to the network in its vicinity. Once this identifier is intercepted, it might be used to retrieve personal information about you.
- Your Ad ID can be accessed by apps and websites on your phone. While it is not directly associated with your personal information (e.g. your name and address), it can be associated with other data such as your location. Some data brokers obtain massive amounts of data from phones and sell it to the police, including the Ad ID.
- Other unique identifiers such as your MAC address can be collected by wifi hotspots but it is far more difficult to associate this with personal information that can be used to identify you.

How to limit the risk of being identified through your 'unique identifiers'

- If you are in a situation, such as a protest, where you may want to ward off the risk of an IMSI catcher tracking your phone, the most effective option would be to refrain from connecting to the cellular network. Having your phone in airplane mode or in a faraday cage will make you invisible to cellular towers, and therefore to IMSI catchers as well.
- If it's important that you are connected to the cellular network, consider getting a separate prepaid SIM card, (because you provide very little information when you buy a pre-paid SIM card). If you do so, note that if your phone connects to a police IMSI catcher at different times with these different SIM cards, it will be possible to tie the pre-paid SIM to the identity registered under your original SIM card. This is because of the IMEI, the unique identifier of your phone.
- Renewing your Ad ID on a regular basis is a good way to avoid all your phone activities being gathered under the same ID. You might also want to disable personalised advertising if your mobile offers this option as it will prevent apps and websites from obtaining this identifier.
- Using an Ad Blocker is also a good way to prevent companies from tracking you online and collecting your personal information.