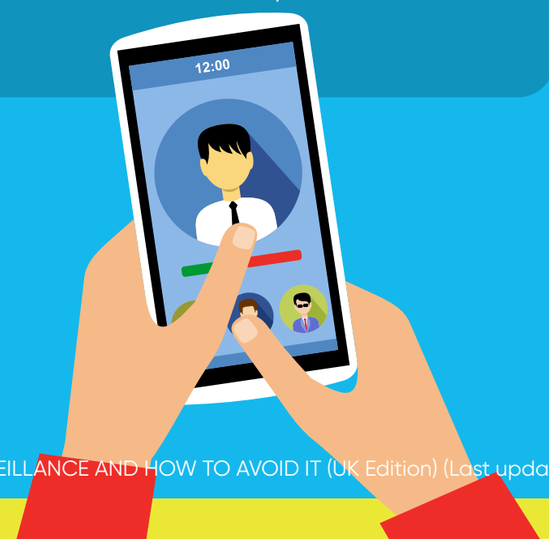
HOW THE POLICE CAN GAIN ACCESS TO YOUR PHONE'S IMAGES, CONTACTS AND DOCUMENTS, AND HOW YOU CAN BETTER CONTROL ACCESS

Where are my images, contacts and documents stored?

- You generate data every time you use your phone e.g. you generate data when you take photographs or record videos, when you create or edit notes and documents on the go, and when you add new names and numbers to your contacts directory.
- All this data is created through dedicated apps - your camera and photo apps, social media apps, notes apps, and your contacts app are just some examples.
- It is important to note that when you create any file on your phone, most of the time you will also generate 'metadata' that is coupled to it (e.g. a photo will have metadata such as the time and location it was shot). This metadata can be as revealing, if not more revealing, than the photo itself.
- All this data will be stored on your phone's internal memory (including any external memory attached, such as a MicroSD card), or on the Cloud, or both if you are using any cloud services as a backup.



How can my images, contacts and documents be accessed by the police?

There are a few ways the police can gain access to this data, depending on how it is stored:

- If you store all your data locally on your phone, then it can be accessed using a 'mobile phone extraction' device, which connects to your phone and downloads all the data stored in it. This method cannot be used remotely - the police would need physical access to your phone.
- Device hacking is an advanced technique that gives access to a certain amount of data in your phone, but not necessarily all of it. Unlike mobile phone extraction, hacking doesn't necessarily require physical access to your device. This means that this method can be used any time before or after a protest.
- If you are syncing your images, documents and contacts using any cloud services (iCloud, Dropbox or Google Drive for example), the police can use 'cloud extraction' tools remotely to access this information without your authorisation or knowledge, or they can make a legal request to the cloud service provider.

How to limit the risk of your images, contact and documents being accessed

- To prevent being targeted by cloud extraction techniques, you would need to refrain from using Cloud services altogether.
- If giving up Cloud services entirely is going to create too much inconvenience for you, consider not uploading sensitive content to the Cloud. Reviewing apps' settings and features is also a good way to ensure you know what data on your phone is being backed-up online (for example, WhatsApp backups can be stored on Google Drive, so even though your WhatsApp messages are end-to-end encrypted, using cloud extraction tools these messages could still be accessed from your Google Drive backup).
- However, as the device user, you have some control over the data you generate in the first place, and where it is stored. Having a good understanding of what information your phone holds about you means that if such tools were to be used on your phone, you are more likely to be aware of what data is being accessed.
- Ensuring the content of your phone is encrypted and that your operating system and apps are up to date will mitigate against some methods of mobile phone extraction and device hacking.