FREE TO PROTEST:

THE PROTESTOR'S GUIDE TO POLICE SURVEILLANCE AND HOW TO AVOID IT



privacyinternational.org

A GUIDE ABOUT POLICE SURVEILLANCE OF YOUR DEVICES











HOW MOBILE PHONE EXTRACTION CAN BE USED AT A PROTEST AND HOW YOU CAN MINIMISE RISKS TO YOUR DATA

What do mobile phone extraction tools do?

- Mobile phone extraction (MPE) tools are devices that allow the police to extract data from mobile phones, including:
  - contacts;
  - call data (i.e. who you call, when, and for how long);
  - text messages (including who you texted and when);
  - stored files (photos, videos, audio files, documents etc);
  - app data (including the data stored on these apps);
  - location information history;
  - wifi network connections (which can reveal the locations of any place where you've connected to wifi, such as your workplace or a café).
- Some MPE tools may also access data stored in the Cloud (so even if you're very careful about minimising data stored on your device, it can still be accessed if it is stored online), or data you don't even know exists, and even deleted data.

How might mobile phone extraction tools be used at a protest?

- The majority of UK police forces have purchased MPE tools and may use them in a range of circumstances, including at protests.
- In order to extract the data stored on it, the police would need to physically access your mobile phone. The police might take your phone if you have been detained, arrested or searched during a protest, but also if you have witnessed or are even the victim of a crime.



What to think about when going to a protest

- Keeping your phone's operating system (Android or iOS) up to date, which means it will have the latest security features, is likely the best way to prevent MPE.
- While the most effective way of protecting yourself against MPE is to not take your phone to a protest, this is unlikely to be a realistic solution. Indeed, not having your phone may leave you vulnerable in other ways.
- While you should keep your phone locked, some MPE tools are reportedly designed to access even locked phones. Their ability to bypass this security does, however, depend on the phone and its operating system.
- Before going to a protest, you may want to consider backing up your phone data to your computer, and then removing that data from your phone. But you should be aware that some MPE tools are able to recover deleted data. If you have saved the data onto a cloud service, some MPE tools can still access that data.

HOW ‘CLOUD EXTRACTION’ TOOLS CAN BE USED AT A PROTEST AND HOW YOU CAN MINIMISE RISKS TO YOUR DATA

What are ‘cloud extraction tools’ and what do they do?

- Cloud extraction technology enables the police to access data stored in your ‘Cloud’ via your mobile phone or other devices.
- The use of cloud extraction tools means the police can access data that you store online. Examples of apps that store data in the Cloud include Slack, Instagram, Telegram, Twitter, Facebook and Uber.

How might cloud extraction tools be used at a protest?

- In order to extract your cloud data, the police would need to physically access your mobile phone. The police might confiscate your phone if you have been detained or arrested during a protest, but also if you have witnessed a crime and even if you are a victim of a crime (See also Protest Guide about mobile phone extraction).
- All of this information could be used to identify protesters and organisers and find out about the location of protests and actions.
- Your cloud data does not just reveal information about you, it can also reveal much about your friends, family, and anyone else you interact with online, such as fellow protestors. For example, you may have old contacts stored in the Cloud, which have been deleted from the phone itself.

What to think about when going to a protest

- While you could consider leaving your phone at home, if that is not a realistic solution, you should think about switching off cloud back-up in the applications on your phone that you use, and logging out of all cloud-based services. This will avoid data being stored in the Cloud and prevent access to this data from your mobile phone.
- Before going to a protest, you should be aware that even if you use end-to-end encrypted messaging through WhatsApp, if you back up your WhatsApp messages to the Cloud, these encrypted backups could be accessed by the police using cloud extraction tools on your phone.
- Some applications, such as Uber, Twitter, WhatsApp and Facebook will allow you to switch off the location data being stored in the Cloud. This may prevent the police being able to track where you have been.



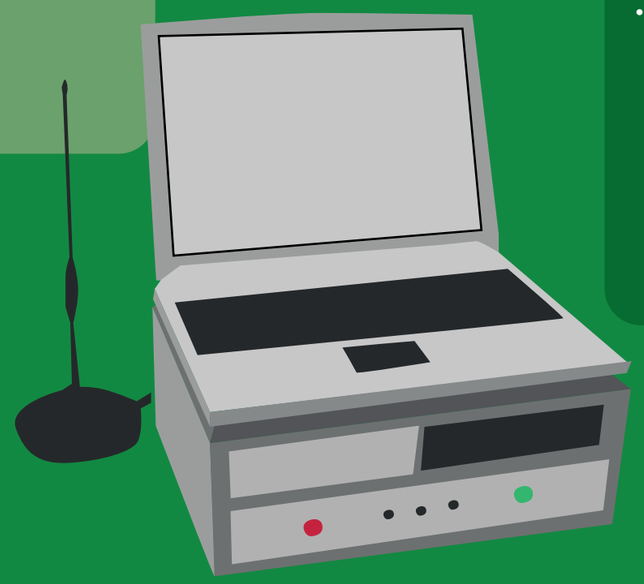
HOW IMSI CATCHERS CAN BE USED AT A PROTEST AND HOW YOU CAN MINIMISE RISKS TO YOUR DATA

What is an IMSI catcher?

- 'IMSI' stands for 'international mobile subscriber identity', a number unique to your SIM card. IMSI catchers are also known as 'Stingrays'.
- An 'IMSI catcher' is a device that locates and then tracks all mobile phones that are connected to a phone network in its vicinity, by 'catching' the unique IMSI number.
- It does this by pretending to be a mobile phone tower, tricking mobile phones nearby to connect to it, enabling it to then intercept the data from that phone to the cell tower without the phone user's knowledge.
- The most accessible information about you in this situation is your location. It is unavoidable that cell towers know your rough location through triangulation - indeed, this is how they provide you with their service in the first place. By putting itself between you and the cell tower, an IMSI catcher can work out your rough location.
- IMSI catchers do not read data stored on a phone. Instead, these devices can be used to try to intercept text messages and phone calls.
- Depending on the IMSI catcher's capabilities and on the network your phone is connecting to, more advanced attacks could take place, even though this is unlikely. Some Stingray devices rely on known weaknesses of communication protocols and can force your phone to downgrade the protocols it is using, to make your communications less secure and more easily accessible (e.g. by downgrading communications over 3G to 2G, because as far as we know, content interception and real-time decryption can only be performed when the target is connected over the 2G network).
- IMSI catchers cannot read the contents of encrypted messages you exchange through platforms that use end-to-end encryption (e.g. Signal, WhatsApp, Wire).

How might IMSI catchers be used at a protest?

- The police can use IMSI catchers to identify who was at a protest, by capturing the IMSI numbers of all the phones that were in its vicinity at that protest.
- Some types of IMSI catchers can even enable the police to disrupt or prevent protests before they even happen.
- For example, they can be used to monitor or block your calls and messages; edit your messages without your knowledge; or even write and send someone messages pretending to be from you.[1]



What to think about when going to a protest

- Putting your phone into airplane mode or switching it off completely will mean that an IMSI catcher can't track you or your communications.
- If you want to prevent the content of your text messages being tracked by an IMSI catcher, you can use messaging services that use end-to-end encryption, such as Signal and WhatsApp. The only information an IMSI catcher could potentially collect is the fact that you are using these messaging apps, not the content itself.
- While IMSI catchers do not read data stored on the phone, do bear in mind that the police have other technology that does enable them to access data on your phone, such as 'mobile phone extraction' and hacking tools.

[1] We don't know for sure whether British police forces are currently using IMSI catchers with these kinds of capabilities. As police forces 'neither confirm, nor deny' the use of IMSI catchers, it's hard to know what type they are using.

HOW SOCIAL MEDIA MONITORING CAN BE USED AT A PROTEST AND HOW YOU CAN MINIMISE RISKS TO YOUR DATA

What is social media monitoring?

- Social media monitoring refers to the monitoring, gathering and analysis of information shared on social media platforms, such as Facebook, Twitter, Instagram and Reddit.
- It may include snooping on content posted to public or private groups or pages. It may also involve "scraping" – grabbing all the data from a social media platform, including content you post and data about your behaviour (such as what you like and share).
- Through scraping and other tools, social media monitoring permits the collection and analysis of a large pool of social media data, which can be used to generate profiles and predictions about users.

How is social media monitoring used in relation to protests?

- Protest organisers will often use social media to organise protests, communicate with protestors, and upload photos and videos of protests.
- In turn this means the police can 'data mine' social media pages and groups to learn the identities and affiliations of the organisers, the location and timing of a planned action, and other related information.
- The police may track social media posts relating to past or future protests to identify protesters.
- The police might also apply facial recognition technology or gait recognition technology to protest images and videos uploaded to social media to identify protestors.

What to think about when going to a protest

- If you upload your protest images to your social media accounts, they may be used to identify and place individuals at the scene of a protest.
- If your location settings are switched on for your social media platforms or your camera and photo apps, and you then post online from or near the site of a protest, police may gain access to that location data.
- If you want to use social media while at a protest, you should consider switching off your location settings on the platform(s) you will be using. If you do decide to share protest images, do not tag individuals that were involved in the protest without their consent, as this could create a trail that police may rely on to place people at the protest.
- If you want to upload your protest images to social media accounts, consider removing the EXIF data beforehand. EXIF data is metadata associated with your images that can reveal information such as the location, time and date and device used.
- Be wary, footage can still be geolocated from background information (e.g. a monument or landmark). Keep this in mind when filming your surroundings and try to avoid identifiable backgrounds.



HOW HACKING CAN BE USED AT PROTESTS AND HOW YOU CAN MINIMISE RISKS TO YOUR DATA

What is hacking?

- Hacking refers to finding vulnerabilities in electronic systems, either to report and repair them, or to exploit them.
- Hacking can help to identify and fix security flaws in devices, networks and services that millions of people may use. But it can also be used to access our devices, collect information about us, and manipulate us and our devices in other ways.
- Hacking comprises a range of ever-evolving techniques. It can be done remotely, but it can also include physical interference with a device or system – for instance by forcing a mobile phone to unlock.
- It can also involve taking advantage of people to gain access to their technology. An example would be 'phishing', where an attacker impersonates a trusted person or organisation to send a link or attachment infected with malware.

How can hacking be used at protests?

- The police are able to hack into communications through the use of, for example, 'IMSI catchers'. But IMSI catchers can only intercept information that is being transmitted between a mobile device and a cell tower; IMSI catchers can't access information that is stored on the device.
- So the police can use sophisticated hacking techniques to get remote access to information stored on a phone, laptop or other internet-connected device used to organise or participate in protests, even if they are secured with a password, fingerprint or face unlock.
- The police may also collect and gain access to any devices that are dropped, lost or confiscated from protesters at a protest.



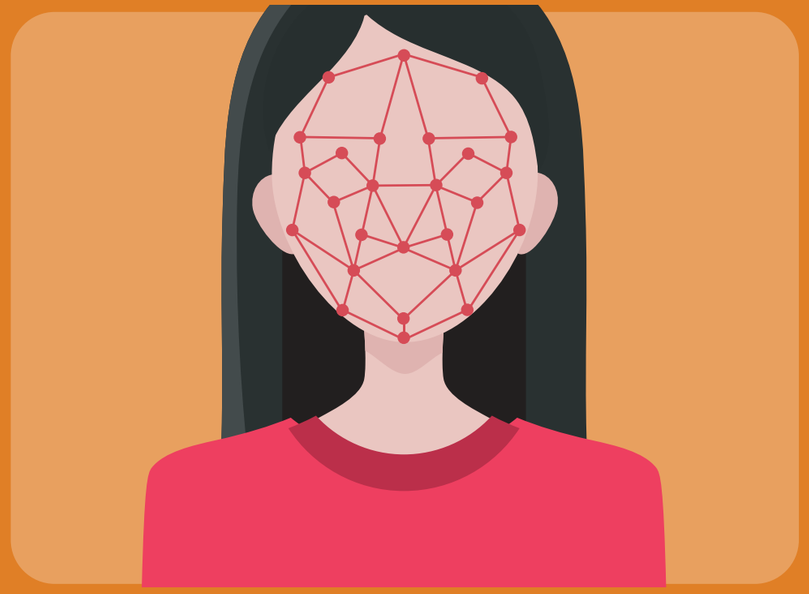
What to think about when going to a protest

- Keeping your device up to date is a good way to prevent hacking, as hacking often exploits vulnerabilities that have been disclosed but not yet patched.
- Ensure that your device is running the latest available version of its operating system (Android or iOS) and that all your apps are up to date to improve your security and minimize the risk of hacking.
- While you should keep your phone or other electronic devices locked, some hacking techniques can access even locked devices. Their ability to bypass this security, does however depend on the hacking technique used and the device it targets.
- Before going to a protest, you may want to consider backing up your phone data to another device, and then removing that data from the devices you take with you. But you should be aware that some hacking tools are able to recover deleted data. If you have saved the data onto a cloud service, some hacking tools can still access that data.
- You should always be careful about what links you click, to avoid 'phishing' attacks.

A GUIDE TO SURVEILLANCE OF YOUR FACE AND BODY











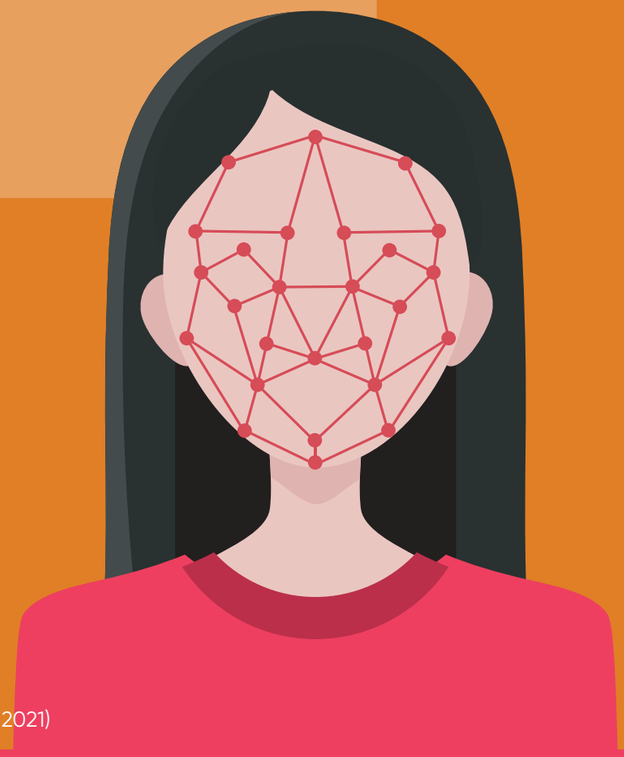
HOW FACIAL RECOGNITION TECHNOLOGY CAN BE USED AT A PROTEST AND HOW YOU CAN TRY TO MAINTAIN YOUR ANONYMITY

What is Facial Recognition Technology?

- Facial recognition technology (FRT) collects and processes data about people's faces, and can be used to identify people. FRT matches captured images with images stored in existing databases or 'watchlists'.

How might it be used in relation to a protest?

- FRT may be used to monitor, track and identify people's faces in public spaces, including at protests. This may be done openly or surreptitiously, without people knowing or consenting.
- FRT-enabled cameras can take pictures or videos, and identify people in real-time or at a later point. FRT can also be used to analyse and identify existing images, for example photos and videos of protests uploaded to social media.
- As protesters' face data is collected, this data can then be added to one or more pre-existing watchlists, where it can be compared against face data from other sources to find a match.
- Such data could also potentially be used to create a new database of people who attend protests for future matching and identification.



What to think about when going to a protest

- If you want to try to maintain your anonymity, you may want to consider wearing a face covering such as a bandana, which may make it harder for FRT to capture accurate images of your facial features.
- Other options for disrupting FRT include the use of face paint and clothes with designs meant to interfere with accurate facial recognition. FRT is constantly changing and improving, however, so face coverings and these other methods may prove less effective in the future.
- Police powers to demand the removal of such coverings and clothing vary depending on the context and jurisdiction. At the time of writing, we are in the midst of the Coronavirus epidemic, so current rules may be subject to change.
- As the police can use FRT to analyse images or video recordings on social media, consider this carefully before you post any images from a protest that feature the faces of other protestors.
- As such, you may want to consider using face blurring tools before posting photos or videos online.

HOW GAIT RECOGNITION TECHNOLOGY CAN BE USED AT A PROTEST AND HOW YOU CAN TRY TO MAINTAIN YOUR ANONYMITY

What is gait recognition technology?

- Gait recognition technology (GRT) can analyse the shape of an individual's body and the unique way in which that body moves when walking or running, which can then be used to identify them.
- GRT works in a similar way to facial recognition technology. But the two main differences are:
  - –GRT may be used at a fairly long range (at the time of writing, about 165 feet / 50 metres), unlike FRT which generally requires more close up, detailed facial images.
  - –GRT can also accurately identify an individual even when that person's facial features are covered, as it doesn't actually rely on 'face data' at all.

How might it be used during a protest?

- GRT could be used to monitor, track and identify people by the shape of their bodies and how they move in public spaces, including at protests, without people knowing or consenting.
- GRT can be used to take pictures or record videos, and identify people in real-time or at a later point. It can also be used to analyse and identify existing images, for example photos and videos of protests uploaded to social media.
- As protesters' body data gets collected, it can then be added to one or more pre-existing watchlists, where this data can be compared to existing body data from other sources, to try to find a match.
- But it could also potentially be used to create a new database of people who attend protests, for future matching and identification.



What to think about when going to a protest

- As the police can use GRT to analyse images or video recordings on social media, consider this carefully before you post any images or video recordings from a protest that feature other protestors.
- To a certain extent, it is possible to disguise your body shape by, for example, wearing baggy clothes, but GRT is sophisticated enough to pick up the unique movement of different people even under such disguises. Similarly, changing how you walk by, for example, faking a limp, will not be sufficient to fool a GRT system.



HOW BODY WORN VIDEO CAMERAS CAN BE USED AT A PROTEST

What do Body Worn Video cameras do?

- Body Worn Video (BWV) cameras can be attached to a police officer's clothing – often at chest, shoulder or head level – and record video, including sound, from the officer's perspective.
- BWV cameras will probably be visible to you, and when it's recording, a flashing light should appear on the device.

How might body worn video cameras be used at a protest?

- BWV cameras may be used at protests to monitor actions of protestors.
- They do not usually capture the police officer's own actions.
- Outside the context of protests, BWV cameras are normally switched on only at the start of an incident. But at a protest, they may remain switched on throughout.
- Some cameras require the video to be uploaded to a server manually afterwards, but some newer BWV cameras enable the footage to be live streamed back to a police station.
- The footage may be processed afterwards, for example, by facial recognition software.

What to think about when going to a protest

- While the Met Police, for example, claim that BWV cameras act as an 'independent witness', individual police officers are able to switch the cameras on and off or decide where to direct the camera, so they are in control of what they record - and don't record.
- See our separate 'Free to Protest' guide to Facial Recognition Technology, regarding the processing of BWV camera footage by facial recognition software.



HOW POLICE DRONES TECHNOLOGY CAN BE USED AT A PROTEST AND HOW YOU CAN TRY TO MAINTAIN YOUR ANONYMITY

What are police drones?

- Drones are remotely controlled Unmanned Aerial Vehicles (UAVs) of varying sizes.
- They usually come equipped with cameras and might be enabled with Facial Recognition Technology.
- Drones can be equipped with speakers, surveillance equipment, radar and communications interception tools, such as 'IMSI catchers'.

How might drones be used during protests?

- Camera-enabled drones may be used to remotely monitor and track people's movements in public spaces, including at protests, without them consenting or even knowing.
- Similarly, when equipped with communication interception technologies, drones can be used to monitor and track protestors' calls and messages, in and around the area where a protest is taking place.
- Drones equipped with speakers may also be used to communicate with protesters, for example by giving them orders, instructions or warnings.[1]

What to think about when going to a protest

- Drones use and impact on with your anonymity depends on the technologies they are equipped with.
- See our 'Free to Protest' guides about Facial Recognition Technology and IMSI catchers, as these are common tools that a drone could use to monitor the activities of protestors.





[1] We don't know for sure what kinds of capabilities the drones used by British police forces are equipped with.

A GUIDE TO POLICING DATABASES AND PREDICTIVE POLICING TOOLS





HOW THE ‘LAW ENFORCEMENT DATA SERVICE’ (LEDS) CAN BE USED AT PROTESTS

What is LEDS?

- LEDS is a new mega-database currently being developed by the Home Office.
- LEDS will replace and combine the existing Police National Database (PND) and the Police National Computer (PNC). The aim is to provide police and others with a super-database, with on-demand, at the point of need access, containing up-to-date and linked information about individuals’ lives.
- Once your details are in LEDS, numerous agencies will have access to that information (e.g. HMRC and DVLA), which can then be utilised in a way that could negatively affect individuals’ lives, employment, state benefits and immigration status.

How might LEDS be used at a protest?

- If you are stopped at a protest by the police, officers will be able to search for your details in the LEDS database (once it is operational). This will provide much more information to the police on a single interface than they have ever had before. Information held about you on LEDS could include your immigration status, driving license information, and intelligence previously gathered about you.
- Police officers will be able to create a record about you in the LEDS database if a prior record does not already exist.
- Further, images that are stored in LEDS may also be used as watchlists, which police can use at protests. Once operational, images from LEDS may also be analysed by facial recognition technology, further enhancing the police’s ability to identify people at protests.

What to think of before you go to a protest

- At the time of writing (Spring 2021), LEDS is not yet operational, so it is unlikely to affect your attendance at a protest for the time being. The Home Office expects the first stage of LEDS to be operational by late 2021.
- However, you need to be aware that the police may still record your details in other databases, such as the PNC and the PND, which will later become part of LEDS.
- You should also be aware that LEDS will not be open for public access and therefore individuals whose information is contained in the system may not have any knowledge that such an entry exists, let alone be able to correct any errors.



HOW PREDICTIVE POLICING CAN BE USED AT PROTESTS

What is predictive policing?

- Predictive policing programs are used by the police to estimate where and when crimes are likely to be committed – or who is likely to commit them. These programs work by feeding historic policing data through computer algorithms.
- For example, a program might evaluate data about past crimes to predict where future crimes will happen – identifying 'hot spots' or 'boxes' on a map. But the data these programs use can be incomplete or biased, leading to a 'feedback loop' – sending officers to communities that are already unfairly over-policed.
- Other predictive policing programs may suggest how people will behave. These programs are fed information about a person, and then they decide whether that person is likely to commit an offence.

How is predictive policing likely to be used in protests?

- The police may use facial recognition technology, IMSI catchers or geo-location technology to identify protesters and add them to databases or watchlists.
- Individuals are also often unaware if they have been included on a Police database or a watchlists and as a result, their removal from it is very difficult, if not impossible.

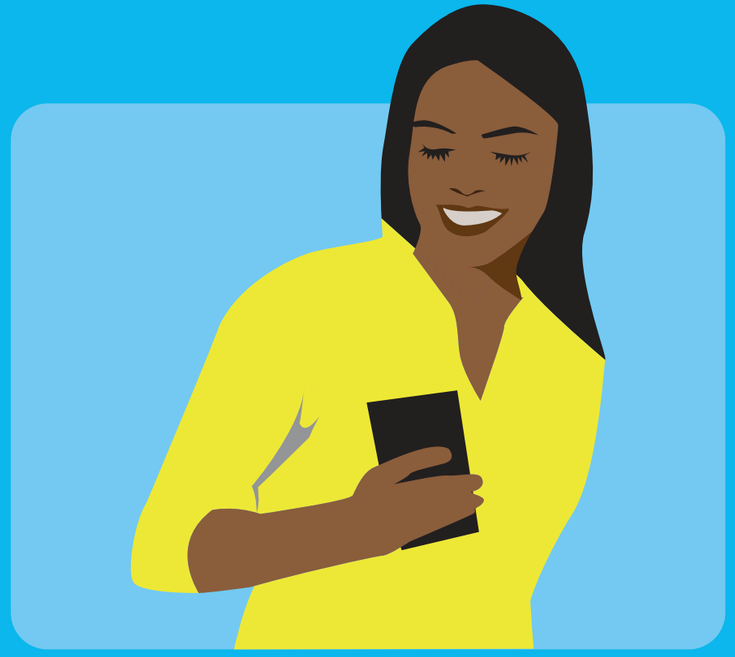
What to think about when going to a protest

- Any photos, videos or messages that you share about a protest on any online platform may be analysed by the police to identify protesters. Once identified, they can then be added to watchlists or used to create profiles that then can feed into predictive policing tools.
- If police have already classified you as someone that is likely to commit a crime, this may further be used to detain, arrest, or stop and search you during a protest.



A GUIDE TO PROTECT YOUR DEVICES AGAINST SURVEILLANCE







74z6j20m
f36rq928

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).



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.

HOW THE POLICE CAN ACCESS YOUR DIGITAL COMMUNICATIONS, AND HOW YOU CAN BETTER CONTROL ACCESS

Where are my communications stored?

- Text messages/phone calls: Traditional cellphone communications happen over the cellular network. You usually access those with the text message and phone call apps that are provided as standard on your phone. While phone calls aren't stored anywhere, text messages are stored locally on your and the recipient's devices. They might also be temporarily stored by the network provider.
- Messaging apps: Messaging platforms enable fairly secure communication over the internet. Depending on the app you use, your messages might be stored locally on your and the recipient's phone, on the service provider's systems, and potentially online too. Some messaging apps also offer backup solutions which will be stored either online or locally. Different messaging apps also rely on different protocols, which means that some messaging apps are more at risk of interception than others.
- Social networks: Except in rare cases of decentralised/self-hosted systems, your communications on social networking apps will be stored by the service providers.



How can my communications be accessed by the police?

There are a few ways the police can gain access to this data, depending on where you have it stored:

- Accessing the communications stored on your phone (such as your conversations in a text messaging app) can be done through a 'mobile phone extraction' device, which can be connected to your phone to download all the data stored on it.
- Such access may also be possible with device hacking, a technique which may not require physical access to your phone.
- If your communications rely on a service provider or a social network (such as Messenger, Telegram, Instagram, TikTok), the police can gain access through 'cloud extraction' technologies, without your consent or knowledge. The same technique can be used to access backups of your communication (e.g. WhatsApp backups on Google Drive/iCloud).
- If some of your communications on social networks are public (e.g. shared on an open Facebook group), the police can also use Social Media Intelligence (SOCMINT) tools to access them.
- Your text messages and phone calls can be intercepted, recorded and interfered with by the police using an 'IMSI catcher', a device deployed to track all mobile phones switched on and connected to the network in a specific area.
- Your text messages can also be accessed through a legal process targeting your service provider. Similar legal processes can be used to request data from companies that might host your communications (e.g. Facebook).

How to limit the risk of your communications being accessed

- Limiting the risks starts with controlling the amount and type of information you share, with whom and through which medium.
- When sharing very sensitive information, consider meeting in person.
- If meeting in person is not an option, given the low security of cellular networks, consider the use of secure channels such as end-to-end encrypted messaging apps to share sensitive information.
- But do bear in mind that if you use cloud backup for any of your messaging apps, the content could still be accessed using cloud extraction tools.
- Verify the identity of protestors you are communicating with through a different communications channel (e.g. messaging them on another platform, or over encrypted email, or over a voice or video call).

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.

FACT SHEET ON YOUR DATA RIGHTS IN RELATION TO POLICE SURVEILLANCE AT PROTESTS



FACT SHEET ON YOUR DATA RIGHTS IN RELATION TO POLICE SURVEILLANCE AT PROTESTS

This is based on UK data protection legislation. The UK's General Data Protection Regulation (UK GDPR) does not apply to processing of personal data for law enforcement purposes by relevant authorities.

What can happen to my personal data at a peaceful protest?

- The most common personal data processed at a protest are notes and photographs taken by police officers, along with voice and video recordings taken from body-worn cameras or drones.
- Data processing can also happen with sophisticated surveillance tools and techniques that you might not be aware of, including facial recognition technology, mobile phone extraction, IMSI catchers and hacking.
- There is no requirement that the protest be violent or at risk of becoming violent before data processing can begin. Moreover, the police are not limited to processing data in relation to preventing offences at the protest. For example, they may process data for the purpose of identifying individuals who are subject to an arrest warrant unrelated to the protest.
- The police do not have to obtain your consent before processing your data.

Are there limits on what the police can do when it comes to my data?

- The police can process personal data at protests, but there are limits. They have to be exercising law enforcement functions and it has to be necessary for the administration of justice (or any other function of a public nature).[1]
- When it comes to sensitive data, like facial images which could be used to identify an individual, the data can only be processed where it is strictly necessary for the administration of justice.[2]
- There are also some forms of data processing that can amount to an interference with the human rights of individuals attending the protest, specifically the right to private life.[3] In order for the police to justify the interference it must be proportionate to the objectives of maintaining public order and preventing or detecting crime.[4] The use of facial recognition technology is one example of data processing which might violate human rights if the proportionality criteria have not been met.[5]
- The police must conduct a Data Protection Impact Assessment before processing data in a way which presents a high risk of violating individual rights.[6] Although there is no legal obligation to publish the assessment, many police forces do so on their websites.
- Police may only hold data for as long as it is necessary to do so.



1. Data Protection Act 1998, Schedule 2(5)
2. Data Protection Act 2018, Section 35
3. Human Rights Act 1998, Schedule 1, Article 8 ECHR
4. R (Catt) v Commissioner of Police of the Metropolis [2015] 1 AC 1065; [2015] UKSC 9 at [17]
5. R (Bridges) v Chief Constable of South Wales Police [2020] 1 WLR 672; [2019] EWHC 2341 (Admin)
6. Data Protection Act 2018, Section 64

Do the police have to inform me that they are processing my personal data?

- Police must make information about their data processing activities generally available to the public.[7] This includes general information necessary for accessing your data and making a complaint about how the police have processed your data. But they don't need to tell you more than that.
- The police are not required to provide notification to you each time they process your data.

Can I see the personal data that was collected on me by the police?

- Individuals can request access to the data about them held by the police. The police must respond by providing access to the data without undue delay and at the latest within one month of receiving the request.[8]
- In addition to receiving the actual data, individuals are entitled to information about the data, including the purposes for which it is held and who it has been disclosed to.
- Individuals have the right to access data about them held by the police, including the right to information about whether the police have processed data about the individual.[9]

What happens if the police refuse to tell me what data they have collected about me?

- The police may refuse to disclose data they have retained about you where it is necessary to protect investigations or prosecutions, protect national or public security and to protect the rights and freedoms of other people.[10]
- Ordinarily the police must provide reasons for refusing to disclose the information, unless providing reasons would undermine the purpose of refusing to provide the information.
- The police may also refuse to disclose data which has been deleted in accordance with the law.[11]

What happens if the personal data held by the police is inaccurate

- Individuals have a right to have their personal data rectified if it is inaccurate or incomplete.[12] If the individuals make a request to have data about them corrected, then the police must fix the inaccuracy without undue delay although there is no fixed deadline.

I'm worried that the police unlawfully processed my data/ unfairly restricted my rights. What can I do?

- You can make a complaint to the police force which processed your data or to the Information Commissioner's Office.[13] In every decision made about your data and communicated to you by the police, you should be provided the contact details of the ICO.

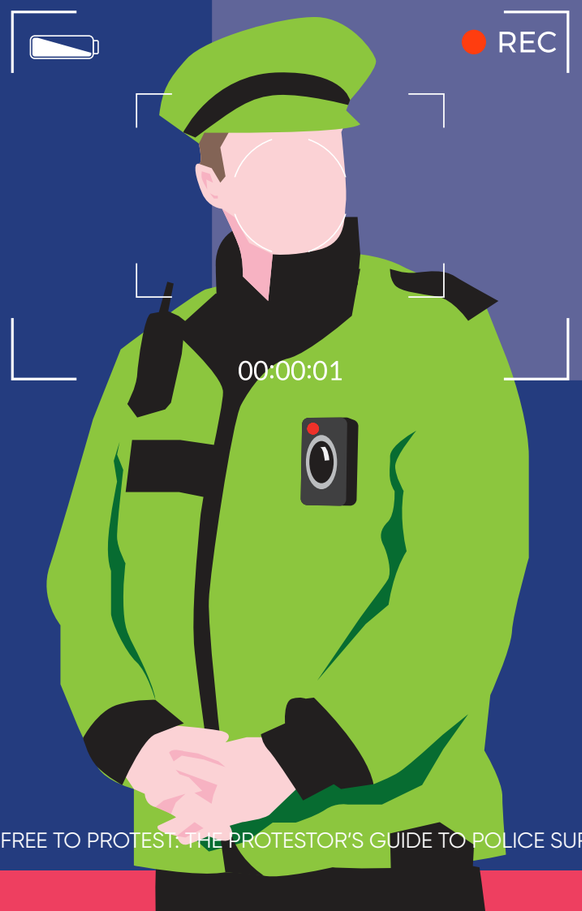
7. Data Protection Act 2018, Section 44
8. Data Protection Act 2018, Section 45(3), Section 54
9. Data Protection Act 2018, Section 45
10. Data Protection Act 2018, Section 45(5)
11. Data Protection Act 2018, Section 39(1)
12. Data Protection Act 2018, Section 46
13. Data Protection Act 2018, Section 165

FACT SHEET ON PHOTOGRAPHING POLICE OFFICERS AT A PROTEST



FACT SHEET ON PHOTOGRAPHING POLICE OFFICERS AT A PROTEST

Photographing or filming incidents involving police and protestors is an important way of holding the police to account for their actions. Members of the public and the media do not need a permit to film or photograph in public places and police have no power to stop them filming or photographing incidents or police personnel.[1]



Can the police stop and search me for filming or taking photographs?

- The police have the discretion to ask you to move back if they think you are interfering with their operations. If you refuse, you can be charged with an offence if your actions amount to obstructing an officer in the execution of their duty.[2]
- A police officer can stop and search you if they have reasonable suspicion that you are carrying illegal drugs, stolen property, a weapon, or a tool that could enable you to commit a crime.[3] In the absence of this reasonable suspicion, an individual can refuse the search.
- But police officers also have the power to stop and search anyone who they reasonably suspect to be a terrorist. This includes the power to view digital images or videos on your phone or camera, to ascertain whether your images or videos constitute evidence that you are involved in terrorism.[4]
- Police officers have the power to seize items found during a search under the Terrorism Act, including a phone or camera, if they reasonably suspect that it constitutes evidence that an individual is involved in terrorism. But they have no right to delete any images or videos.
- Police officers can also question an individual who appears to be taking photographs of someone who is or has been a member of Her Majesty's Forces or Intelligence Services as long as this is being done for a lawful purpose and is not being done in a way that prevents, dissuades or inhibits the individual from doing something which is not unlawful.[5]

Are there limits to how images can be used?

- It is an offence to publish or distribute a photograph of a police officer, member of the armed forces or security services, if it is likely to be useful to a person preparing any act of terrorism.[6]
- If you are publishing your photos from a protest online, including on social media, bear in mind that the police may be able to use those photos to identify individuals present at a protest.

1. https://www.met.police.uk/advice/advice-and-information/ph/photography-advice
2. Section 89(2) of the Police Act 1996
3. Section 1 of the Police and Criminal Evidence Act 1984
4. Section 43 of the Terrorism Act 2000
5. Section 58A of the Terrorism Act 2000[17] Section 89(2) of the Police Act 1996
6. Section 76 of the Counter-Terrorism Act 2008

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).