LIBERTY

PRIVACY INTERNATIONAL

NEIGHBOURHOOD WATCHED

How policing surveillance technology impacts your rights

MOBILE PHONE EXTRACTION

WHAT IS MOBILE PHONE EXTRACTION?

Mobile phone extraction tools are devices that allow the police to download data from mobile phones, including:

- Contacts.
- Call data – who we call, when, and for how long.
- Text messages.
- Stored files – photos, videos, audio files, documents, etc.
- App data – what apps we use and the data stored on them.
- Location information.
- Wi-fi network connections – which can reveal the locations of any place where we've connected to wi-fi, such as our workplace and properties we've visited.

Some mobile phone extraction tools may also access data stored in the cloud instead of directly on our phones, or data we do not know exists or cannot access. For instance, mobile phones may contain data we believe was deleted.

WHAT IF MY PHONE IS LOCKED?

Mobile phone extraction tools are designed to access locked phones, although their ability to do this will depend on the phone and its operating system.

Mobile phone extraction tools may access locked phones by exploiting security vulnerabilities in the phone. For that reason, the use of these tools may constitute a form of "hacking".

When police use these tools, they are making a choice to leave our phones insecure, which make them an easier target for attacks by other people. So if the phone is later returned to the owner, it may be unsafe for use.

WHO IS USING MOBILE PHONE EXTRACTION TOOLS?

The majority of police forces have purchased mobile phone extraction tools.

In March 2018, Privacy International uncovered that 26 out of 47 UK police forces use mobile phone extraction – and three were about to trial it for the first time.

The police might take your phone to extract data if you have been arrested, but also if you have witnessed a crime or are even the victim

WHAT ABOUT MY RIGHTS?

Privacy

Mobile phone extraction allows the police to access and download all of the data stored on your mobile phone. For most people, this will include the most private information they store anywhere, including their contacts, messages, web browsing history and banking information.

Some tools can also download data stored in the cloud, which may include app-based data, including for popular platforms like Facebook, Google, Twitter, Instagram and more.

The information accessed by the police will not only relate to you, but will contain personal data, such as messages or photos, related to family, friends and colleagues. The police may store all of this data indefinitely and combine it with other information they hold to build up an even more intrusive picture of our lives.

WHAT DOES THE LAW SAY?

The law gives the police the power to use mobile phone extraction tools – but it is unclear exactly what authority the police are actually relying on.

Mobile phone extraction could be covered by the "equipment interference" power in the Investigatory Powers Act 2016 but Privacy International has discovered the police are relying on other laws to engage in this form of hacking.

This lack of clarity is concerning because different legal authorities contain different rules and safeguards for intrusive policing activities. For example, the Investigatory Powers Act requires that police obtain a warrant before using equipment interference powers.

In general, the police appear to be conducting mobile phone extraction without seeking a warrant.

HAVE YOUR SAY ABOUT MOBILE PHONE EXTRACTION

Each police force across England and Wales has an elected Police and Crime Commissioner (PCC). PCCs should be a vital way for the local community to hold their local police force to account. Your PCC should listen to and represent your views about how the police work in your area.

Find out who your local PCC is and how to contact them here. In Scotland, you can contact the Scottish Police Authority.

LIBERTY

libertyhumanrights.org.uk

PRIVACY INTERNATIONAL

privacyinternational.org