LIBERTY

PRIVACY INTERNATIONAL

NEIGHBOURHOOD WATCHED

How policing surveillance technology impacts your rights

HACKING

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.



WHO IS HACKING?

A range of private companies and public sector bodies are known to use hacking techniques.

For example, the majority of UK police forces have purchased technology to conduct "mobile phone extraction", which allows them to download all of the data from your phone, including contacts, text messages and photos.

Though the police "neither confirm nor deny" their use of other hacking methods, it has been revealed that various police forces have deployed remote hacking techniques to carry out secret surveillance.

But by exploiting vulnerabilities instead of reporting and helping to fix them, the police are leaving our devices, networks and services insecure – making them an easy target for criminals.

WHAT DOES THE LAW SAY?

The law does give police the power to hack. They can carry out "equipment interference" under the Investigatory Powers Act (IPA) and "property interference" under the Police Act 1997.

The police can use the powers in the IPA to hack for surveillance purposes, such as obtaining our communications and data.

The Police Act lets them hack for other purposes, such as to disrupt or disable a system.

The IPA also gives a range of additional law enforcement bodies the power to hack for surveillance purposes – including immigration officers, Revenue and Customs officers, and Competition and Markets Authority officers.

Liberty is challenging the hacking powers in the Investigatory Powers Act in the courts through the People vs The Snoopers' Charter legal challenge.

Privacy International is also challenging the hacking powers of GCHQ in the courts.

WHAT ABOUT MY RIGHTS?

Privacy

Hacking allows the police to access all of the data stored on the systems that they hack. Personal digital devices contain some of the most private information we store, including our contacts, communications, diaries, photo albums and financial information.

Hacking also permits the police to conduct real-time surveillance. They can secretly and remotely turn on a device's microphone, camera, and GPS-based locator technology.

The police may also capture screenshots of the hacked device and see login details, passwords, internet browsing histories, documents and communications.

Fair Trial

Where evidence is obtained by hacking, it may interfere with your fair trial rights. Hacking permits the police to manipulate data on systems in a variety of ways, including by planting, corrupting or deleting data, sending data from the target system, or recovering data that has been deleted.

This manipulation may also be an unintentional result of hacking.

HAVE YOUR SAY ABOUT HACKING

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