Equipment Interference

EQUIPMENT INTERFERENCE (EI) is the term given in the Investigatory Powers Act to describe the process of hacking. The police and the intelligence agencies; MI5, MI6 and GCHQ are legally allowed to hack a device such as a computer, laptop, mobile phone, tablet or internet connected device, system or network in order to watch, change, destroy or obtain data in secret without the user knowing.

What concerns are there?

Equipment interference is the process of accessing a device, system or network in order to:

- Use the device to hack or infect other machines, networks or systems.
- Remote control a camera or microphone.
- Access files and read encrypted data.
- Access private passwords or encryption keys.
- Monitor internet activity in real time.
- Potentially destroy the device.

Equipment Interference is a method used to work around encryption. By going straight into a device the encryption used to protect communications becomes meaningless as everything will be clearly readable. Encryption protects communications in transit. For more information see our Encryption Factsheet.

Targeted or Bulk?

The Act permits two types of Equipment Interference warrant; targeted and bulk.

Targeted equipment interference warrants:

- Are used by the police, intelligence agencies and HMRC.
- Authorise hacking of specific people, locations or organisations.
- But they also authorise the hacking and examination of "more than one location", "a group of persons" or "more than one person or organisation" which means they can be used in a bulk way.

Bulk equipment interference warrants:

- Are used internationally by the intelligence agencies when they do not know exactly who, where or what they want to hack.
- Bulk warrants are used when the necessity and proportionality cannot be clearly determined.
- A bulk warrant authorises hacking for six months.
- If a UK citizen's data is accessed a targeted examination warrant is needed to view the data.

The Intelligence and Security Committee raised concern before the Act became law, that targeted warrants allow for the interference of so many people they make bulk warrants meaningless. Their recommendation that a warrant which impacts a large number of people should be approved for no longer than one month, was dismissed.

Equipment Interference

Can innocent people be lawfully hacked?

Yes, it is called intended intrusion.

Intended intrusion:

- Does not appear on the face of the Act but is described in the code of practice.
- Allows the intelligence agencies to hack completely innocent people who are not the target of interest.
- People can be hacked purely so the intelligence agencies can gather information on the real target they are investigating.

How can a device be hacked?

Hacking can be done in person or remotely using malware to drop a virus onto the device or into the system. You will never know if your device has been infected.

Malware is the term used to describe any type of malicious software such as a virus, spyware, worms or Trojan:

- A virus spreads across machines, systems and networks.
- Spyware sits on a device to monitor and track all activity.
- Worms destroy information and files on a device.
- Trojans pretend to be a normal safe programme but are really a virus. They can be used to steal information and take over files. A Trojan can be used to cripple networks.

There are a number of ways malware can get onto a device but two of the most common are:

Via email: An email is sent containing a link with malware software embedded in it. When the link or attachment is opened the malware is activated.

Via a fake webpage: Malware is activated when the person visits a fake webpage.

What are the risks?

- Open networks and cloud technology make the spread of viruses much easier.
- If the malware is a virus it has the potential to infect other devices, systems or networks making innocent people vulnerable to infection on their machines. This problem is often referred to as collateral interference.
- If an organisation is the target of the hack your personal information, communications or passcodes could be seen.

Don´t forget

- Eqiupment interference is used by the police on UK citizens and by the intelligence agencies in the UK and internationally.
- Targeted warrants are so broad they can be used thematically to hack groups of people.
- Your computer, phone or tablet could be made vulnerable by malicious software.
- You will never know if you have been the target of equipment interference.
- A business or organisation you have innocent dealings with may be the target of a hack.
- It is legal for an innocent person to be hacked to get information on a person of interest.

Investigatory Powers Act Factsheet | BIG BROTHER WATCH