

Interception

INTERCEPTION is the ability to listen in on what someone says or writes. There are two types of interception in the Investigatory Powers Act; targeted and bulk. Targeted is used when the focus of the investigation is known. Bulk is used when the target is unknown. Bulk interception describes the gathering of large chunks of internet traffic from around the world. Because bulk is used to discover rather than investigate it could be described as a form of pre-crime investigation.

What is interception?

Interception allows someone to listen into a phone call, read your online communications be it via the internet or an app; or read the contents of a letter before the letter is delivered.

The police, intelligence agencies and HMRC use interception. The police and HMRC use targeted interception in order to investigate known criminal activity. The intelligence agencies use both targeted and bulk interception.

Difference between targeted and bulk

Targeted:

- This form of interception is used on UK citizens who are suspected of illegal activity.
- It can be conducted on a specific person or a specific location by the police, the intelligence agencies or the armed forces.
- The request must be specific as to who or what will be spied on and where.
- Targeted can also be used in a thematic way. Thematic means groups of people, an area of locations, a number of organisations.

Bulk:

- Is done by tapping internet cables carrying the world's internet traffic.
- The intelligence agencies now have the lawful power to tap these cables and grab chunks of internet activity.
- Bulk interception is broad, rarely based on a specific investigation and is used to look for plots, behaviour or activity which may potentially be of a criminal or terrorist nature.

Should you be worried about interception?

If you are a **law abiding citizen** and you do not communicate with terrorists or criminals it is highly unlikely that you will have targeted interception used on you.

But because of the nature of the internet, the process of bulk interception and the collection of vast chunks of internet traffic to search for potential strange behaviour, leaves all of us who use the internet vulnerable to being caught up in the surveillance net.

Your communications may never be looked at, but there is no guarantee. The idea that we are all a potential suspects may concern some people.

Interception

What are the safeguards?

Warrants are decided on the necessity and proportionality of the request, but the codes of practice for bulk powers make clear that some warrants are approved when the necessity and proportionality cannot be determined.

We are told that communications gathered in bulk are not looked at, that the data is held and analysed using specific search terms, definitions and criteria which pick out only the communications of interest. These search terms, definitions and criteria are unknown.

If a UK citizens communications are caught up in the net of bulk data, a targeted warrant to look at the communication will be required. However, due to the nature of the internet it is not always immediately clear that a communication has a UK focus to it. This protection could in theory be applied after the communication has already been viewed.

Is information from intercept used in court?

No, evidence gathered from interception cannot be used in a UK court of law. It cannot be disclosed, questioned or even hinted at.

Intercept evidence is used in court in the USA, Australia, Canada, New Zealand and South Africa with no negative impact.

Don't forget

- Interception is the process of spying on texts, emails, letters and internet activity or the listening in on telephone calls.
- Targeted intercept is used when the focus of an investigation is known.
- Bulk intercept is used when the precise investigation is unknown.
- Targeted can be used in a thematic way, which means groups of people, organisations or areas can be monitored.
- Bulk interception leaves anyone who uses the internet or a telephone vulnerable to their data being looked at or listened to.
- Evidence gathered through intercept cannot be used in a court of law. It can only be used as part of a secret investigation.