



Investigatory Powers Bill

Key points

- Terrorists, serious criminals and hostile states are using technology which limits the effectiveness of other investigatory techniques such as interception of communications. In order to keep pace with our adversaries the security and intelligence agencies have had to develop new techniques to enable them to gather intelligence and evidence. These techniques include Equipment Interference.
- Bulk Equipment Interference (Bulk EI) is a form of Equipment Interference that collects data relating to a number of devices (for example, devices in a particular area) in order to identify potential targets of interest.
- Bulk EI is reserved for activity with a foreign focus and may only be undertaken by the security and intelligence agencies and only for matters relating to national security.
- As with other bulk powers, strong safeguards will apply to the regime. This means that Bulk EI:
 - will be used only when necessary for a legitimate purpose and proportionate to that purpose,
 - that the data obtained from EI will be stored safely and that once no longer required any information is destroyed securely.
- A double-lock authorisation process will require bulk EI warrants issued by the Secretary of State to be approved by an independent Judicial Commissioner before coming into force. Only a small portion of the data gathered through bulk EI will be selected for examination. An individual warrant will be required for any examination of content of persons in the UK that may be contained within this data.

Background

- Bulk EI facilitates target discovery, it helps to join up the dots between fragments of information that may be of intelligence interest. The individuals identified by this target discovery work may already be known, in which case valuable extra intelligence may be obtained. Or you may uncover previously unknown individuals or plots that would otherwise not have been detected.
- It is possible that bulk activity might capture data and information about UK persons, for instance if they are associated with a subject of interest.
- When an analyst needs to access the data of someone in the UK he or she will first need the authorisation of the Secretary of State and an independent Judicial Commissioner in the form of a separate targeted examination warrant. This process mirrors the procedure that applies to Bulk Interception when the communications of a person in the UK are captured.

Key facts

- GCHQ conducts EI operations with a foreign focus to protect the UK and its interests. In 2013 around 20% of GCHQ's intelligence reports contained information that derived from EI operations against a target's computer or network.
- Equipment interference was avowed by the Government in February 2015 with the publication of a draft Equipment Interference Code of Practice.
- Bulk warrants authorise the use of Equipment interference to obtain and analyse data of persons located outside the UK.
- Bulk EI will provide vital intelligence from sources that would otherwise be unavailable – for instance when a communication is encrypted when transmitted and therefore not available through interception.

Key Quotes

“Changes in the technology that people are using to communicate are making it harder for the Agencies to maintain the capability to intercept the communications of terrorists. Wherever we lose visibility of what they are saying to each other, so our ability to understand and mitigate the threat that they pose is reduced.”

Andrew Parker, terrorism, technology and accountability (RUSI, 8 Jan 2015)

“This task is, of course, becoming more complicated. The evolution of the internet and modern forms of communication provide those who would do us harm with new options; they provide those who would protect us – the police, the security and intelligence agencies, the National Crime Agency and others – with new challenges.”

Home Secretary, Defence and Security Lecture (Mansion House, 24 June 2014)



Investigatory Powers Bill

Why do we need it?

- Equipment interference is used to secure valuable intelligence to enable the Government to protect the UK from individuals engaged in terrorist attack planning, cyber attacks and other threats to national security.
- EI operations may provide information that would otherwise be unobtainable. For instance, when a key piece of information is only transmitted to another device when encrypted.
- Bulk equipment interference allows agencies to take receipt of large quantities of foreign-focussed material and then filter it in order to identify only the data of intelligence value.
- Carefully directed searches of large volumes of data allows the agencies to identify patterns of activity that the agencies would be otherwise be unable to discover. This significantly narrows down the areas for investigation, prioritises intelligence leads, and provides valuable information that can be followed up by MI5 or law enforcement.
- Access to this data is crucial to monitor known and high-priority threats and uncover other identities or communications methods targets may be using. Access to this data is also crucial to discover new and emerging targets.
- Access to large volumes of data is essential to enable fragments of communications or other data relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation.

What is new?

- A clear distinction between targeted and bulk equipment interference including robust safeguards to ensure bulk equipment interference is used proportionately and access to the data is tightly controlled.
- A double-lock authorisation process will require warrants issued by a Secretary of State to be approved by an independent Judicial Commissioner before coming into force.
- Further detail of the safeguards concerning access, retention, storage, destruction, disclosure and auditing of Equipment Interference will be set out in a new Equipment Interference Code of Practice.

What are the safeguards?

- Warrants may only be issued by a Secretary of State where he or she is personally satisfied that the activity would be both necessary and proportionate.
- A 'double-lock' authorisation procedure will be in place requiring warrants issued by a Secretary of State to be approved by a Judicial Commissioner before coming into force.
- Warrants will last up to 6 months. Any extension must be subject to review by the Secretary of State and an independent Judicial Commissioner.
- The material obtained through bulk EI can only be analysed if the reason for doing it relates to an Operational Purpose agreed alongside the warrant. E.g. It might provide for the examination of material providing intelligence on ISIL attack planning against the UK.
- Before material obtained under a bulk equipment interference warrant may be examined, it is subject to another consideration of the necessity and proportionality of so doing.
- In the course of an investigation if the data of someone in the UK needs to be examined the analyst must acquire a separate and additional targeted warrant from a Secretary of State and an independent Judicial Commissioner to examine the material.
- A statutory Code of Practice will set out the handling, retention, destruction and audit arrangements for the data obtained by bulk equipment interference.

Who can do it? When? Under what authorities?

- Due to the potentially greater intrusive nature of bulk equipment interference, it will be limited to the security and intelligence agencies for national security purposes, in the same manner as other bulk powers.
- Warrants can be granted for investigations in to serious and organised crime, the economic well-being of the UK and national security, but national security must always be one of the reasons for acquiring the warrant.