Investigatory Powers Bill

Key points

- Reflecting the Government's commitment to delivering greater transparency, the Home Secretary informed Parliament on 4 November that the Security and Intelligence Agencies are able to acquire communications data in bulk, including domestically, from Communication Service Providers under Section 94 of the Telecommunications Act 1984.
- Fast and secure access to communications data is essential to the security and intelligence agencies in protecting the UK. Communications data has played an important part of every MI5 investigation over the last decade.
- Accessing communications data in this way enables the agencies to join the dots in their investigations, working at pace to detect and disrupt threats to the UK. This has helped stop terrorist attacks, and has saved lives many times.
- The data does not include internet connection records or the content of communications.
- It is held securely and access to it is strictly controlled.
- The acquisition of communications data in bulk is only permitted when it is necessary for the protection of national security. The data is only accessed where necessary and proportionate, to enable the agencies to carry out their statutory functions – it cannot be accessed for other purposes.
- The Bill will strengthen safeguards around acquisition of communications data in bulk, requiring all warrants to be subject to the 'double-lock' of Secretary of State and Judicial Commissioner authorisation.
- The Bill will also repeal the existing Section 94 power.

Background

- There is an existing power for the Secretary of State to issue directions to Communications Service Providers under Section 94 of the Telecommunications Act 1984 which has enabled the Security and Intelligence Agencies to obtain communications data in bulk.
- David Anderson QC recommended that existing and future intrusive capabilities should be publicly avowed as far as national security allows. He also recommended the creation of bulk communications data warrants as part of the overhaul of legislation in this area.
- Exercise of this power is currently overseen by the Interception of Communications Commissioner.

Key facts

- Communications Data has played a key role in all MI5 investigations over the past decade
- The data is used for a variety of purposes, in particular to join the dots in complex and sensitive investigations and to allow the agencies to access data securely and at speed.
- The Security and Intelligence Agencies' use of the Section 94 power has been approved by successive governments and Secretaries of State.
- The Prime Minister made a statement in March 2015 that the Interception of Communications Commissioner provided oversight of the use of Section 94.

"This is a vital power, and its use has been closely guarded until now."
Home Secretary, 4 November 2015

"We use data to save lives. Accessing data quickly, reliably and at scale is as fundamental to our work – whether that is communications data (the 'who' and 'when' of communications, not the 'what'), or whether it is travel data, passport information or other data sets. Data is critical to our ability to identify threats in the first place, and it enables us to join the dots in our investigations to identify those who may be involved in planning attacks." **Andrew Parker, MI5, 28 October 2015**

"*Existing and future capabilities within the scope of this Review…should be publicly avowed by the Secretary of State at the earliest opportunity consistent with the demands of national security*". **David Anderson QC, A Question of Trust, June 2015**

Investigatory Powers Bill

Why do we need it?

- Where a Security and Intelligence Agency has only a fragment of intelligence about a threat or an individual, communications data obtained in bulk may be the only way of identifying a subject of interest.
- Access to large volumes of data is essential to enable the identification of communications data that relates to subjects of interest and to subsequently piece together the links between them.
- Carefully directed searches of large volumes of data also allow the agencies to identify patterns of activity that significantly narrows down the areas for investigation and allows them to prioritise intelligence leads.
- Identifying the links between individuals or groups can also help the agencies to direct where they might request a warrant for more intrusive acquisition of data, such as interception.
- It allows agencies to search for traces of activity by previously unknown subjects of interest who surface in the course of an investigation in order to identify them.

Who can do it? When? Under what authorities?

- Only the Security and Intelligence Agencies (MI5, GCHQ and SIS) will be able to obtain a warrant to acquire communications data in bulk. They must state the operational purposes for which the data can be interrogated.
- 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.
- The Security and Intelligence Agencies will only be able to obtain such a warrant where one of the purposes for acquiring it is national security.
- The interrogation of any data obtained by the agencies under a bulk communications data warrant must be only for specified, operational purposes issued and approved by the Secretary of State and Judicial Commissioner alongside the warrant.

What are the safeguards surrounding its use?

- Bulk communications data powers are limited to the Security and Intelligence Agencies.
- Bulk communications data can only be obtained when it is required to protect national security.
- 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.
- Operational purpose of interrogating data obtained under a bulk communications data warrant to be agreed alongside the warrant.
- Any application for a warrant must contain a consideration of necessity and proportionality.
- Unauthorised acquisition of communications data is an offence under the Bill.
- The Investigatory Powers Commissioner will provide statutory oversight of bulk communications data, including audit and inspection, and publishing annual reports on compliance.
- A statutory Code of Practice will underpin the regime, with details of handling, destruction, retention and examination safeguards.
- For sensitive professions, investigators must give special consideration prior to making any requests for access to data relating to those people they know to be working in sensitive professions. Any access to such data must be recorded and made available to the Commissioner.
- Anyone who believes they have been unlawfully the subject of investigatory powers can complain to the Investigatory Powers Tribunal.

What is new?

- Communications data acquisition powers will be in a single piece of legislation.
- Section 94 of the Telecommunications Act 1984 will be repealed.
- Robust, transparent safeguards including judicial approval of warrants issued by a Secretary of State.
- Bulk communications data can only be obtained in the interests of national security. Operational purposes must underpin the interrogation of data.

Access to domestic bulk communications data has enabled MI5 to thwart a number of attacks here in the UK. In 2010, when a group of terrorists were plotting attacks in the UK, including on the London Stock Exchange, the use of bulk communications data played a key role in MI5's investigation. It allowed investigators to uncover the terrorist network and to understand their plans. This led to the disruption of their activities and successful convictions against all of the group's members.