



# Investigatory Powers Bill

## Key points

- A bulk personal dataset (BPD) is a dataset containing information about a wide range of people, most of whom are not of interest to the security and intelligence agencies. Lists of people who have a passport or a licensed firearm are good examples of a BPD – they include a large amount of personal information, the majority of which will relate to people who are not of security or intelligence interest.
- Use of BPDs are an essential way for the security and intelligence agencies to focus their efforts on individuals who threaten our national security, by helping identify or establish links between such individuals.
- The use of BPDs helps the agencies to focus on the individuals of concern – for example, terrorists and spies – and it removes the need to use more intrusive techniques against the innocent.
- The Bill will provide a ‘double-lock’ authorisation procedure requiring warrants issued by a Secretary of State to be approved by a Judicial Commissioner before coming into force.
- The acquisition and use of the BPD must be necessary and proportionate and measures must be in place to store the datasets securely.
- The safeguards that apply to the security and intelligence agencies’ access, retention, storage, destruction, disclosure and auditing of BPDs will be covered by a statutory Code of Practice.

## Background

- The David Anderson and ISC reviews of investigatory powers said that the safeguards that apply to the security and intelligence agencies’ acquisition and use of BPDs should be placed on a clear statutory basis.
- The acquisition and exploitation of BPDs is an essential building block for the security and intelligence agencies’ investigations.
- BPDs enable the intelligence agencies to join the dots – narrowing down the search to identify specific individuals from fragments of information and early leads – to focus on threats and exclude the innocent and so protect national security, stop terrorists, and counter serious and organised crime groups.
- BPDs vary in size and may be linked together so that analysts can quickly find all the information linked to a specific search query.

## Key facts

- The Security Service Act 1989 and the Intelligence Services Act 1994 provide the legal basis for the acquisition and use of BPDs by the security and intelligence agencies.
- The security and intelligence agencies have robust internal safeguards that govern the acquisition and use of BPDs. Internal access and use of BPDs is tightly controlled by strict handling policies.
- The use of BPDs by the security and intelligence agencies is overseen by the independent Intelligence Services Commissioner. In March 2015 the Prime Minister put this work of the Commissioner on a clear statutory footing and the Commissioner gave details of his role in his annual report in July 2015.

## Quotes

*“The procedures governing use are such that any access can only be justified for a proper business purpose so that intrusion into the privacy of persons not of intelligence interest is avoided. Officers work with a high degree of integrity ... misuse by individuals is rare and treated very seriously”*

**Sir Mark Waller, Intelligence Services Commissioner**

*“The Agencies use Bulk Personal Datasets ... to identify individuals in the course of investigations, to establish links, and as a means of verifying information obtained through other sources. These datasets are an increasingly important investigative tool for the Agencies.”*

**Privacy and Security, Intelligence and Security Committee of Parliament**



# Investigatory Powers Bill

## Why do we need it?

- Legislation will put on a clear footing the safeguards and protections that surround the use of BPDs by the security and intelligence agencies.
- Access to such datasets provides an essential way for the security and intelligence agencies to focus their efforts on individuals or organisations that threaten our national security.
- The agencies acquire and use BPDs to:
  - help identify subjects of interest, or unknown individuals who surface in the course of investigations (and eliminate those who are innocent and unconnected to the investigation without the use of more intrusive techniques);
  - establish links between individuals and groups, or else improve understanding of a target's behaviour and connections; and
  - verify information obtained through other sources e.g. via agents.
- Under the Bill there will be two types of warrant: class warrants, covering particular types of BPDs – such as travel data – and specific warrants, covering a specific dataset.

## What is new?

- The ability to acquire and access BPDs is not a new power for the security and intelligence agencies. It relies on existing powers such as the Security Service Act or Intelligence Services Act. The Bill does the following:
  - Time-limit BPD warrants to a period of six months;
  - Introduce a 'double-lock' authorisation procedure requiring warrants issued by a Secretary of State to be approved by a Judicial Commissioner before coming into force.
- A statutory Code of Practice will replace the newly published Handling Arrangements, which provide robust safeguards for the handling, retention, destruction and audit arrangements of BPDs.

## Who can do it? When? Under what authorities?

- The security and intelligence agencies only ever acquire and use BPDs in accordance with their statutory functions.
- Acquisition and use has to be lawful, necessary and proportionate.
- Within the agencies, staff given access to BPDs must be trained on their legal responsibilities. All searches must be justified on the basis of necessity and proportionality and they are audited to ensure that any misuse is identified. Any staff found to have accessed datasets inappropriately are disciplined and may be dismissed or face criminal prosecution.

## What are the safeguards?

- Secretaries of State will issue warrants authorising the use of BPDs on a six monthly basis.
- The Secretary of State must believe that the warrant is necessary and proportionate and adequate measures are in place to store the datasets securely.
- Before a warrant can be issued, a Judicial Commissioner must approve it.
- In urgent cases (which apply to specific BPD warrants only), a Judicial Commissioner must approve the Secretary of State's decision to issue a warrant within 5 working days, or the warrant ceases to have effect.
- The safeguards that apply to the intelligence agencies' access, retention, storage, destruction, disclosure and auditing of bulk personal datasets will be codified in a statutory open and transparent Code of Practice.
- The new Investigatory Powers Commissioner will oversee compliance with this Code and hold the agencies to account. This will replace the oversight provided by the Intelligence Services Commissioner.
- These measures will clarify the authorising model for acquiring and using BPDs and bring it into line with powers in the Bill.
- As is the case now, datasets must be deleted when it is no longer necessary or proportionate to hold onto them.

*“Using data appropriately and proportionately offers us a priceless opportunity to be even more deliberate and targeted in what we do, and so to be better at protecting...this country”* **Chief SIS, English Heritage speech, March 2015**