Investigatory Powers Bill

Key points

- The Bill updates the definition of communications data in respect of telecommunications services to provide for technologically neutral, modernised definitions.
- The Bill creates, for the first time, a definition of the content of a communication or an item of information.
- New definitions of related communications data and equipment data mean that data acquired under the powers in the Bill can be handled with appropriate safeguards, regardless of the power under which it was acquired.

Background

- Under RIPA communications data is currently broken down into three sub-categories: traffic data, service use information and subscriber information. Any data falling outside these definitions is deemed to be content.
- David Anderson recommended that "*The definitions of content and of communications data, and any subdivisions, should be reviewed… so as to ensure that they properly reflect both current and anticipated technological developments and the privacy interests attaching to different categories of material and data.*"

The New Data Framework

- The Bill replaces the existing framework by creating 3 categories of data: Communications data, Related Communications Data/ Equipment Interference and Content.

<u>Communications data</u>

- Communications data is data held by a CSP or available directly from the network which identifies a person or device on the network, ensures that a communication reaches its intended destination, otherwise describes how communications move across the network or otherwise describes how a person has been using a service.
- It is categorised into:
    - *Entity data* – This data is about entities or links between them but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).
    - *Events data* – Events data identifies or describes events which consist of one or more entities engaging in an activity at a specific point, or points, in time.
- The authorisation levels required to access communications data reflect the fact that the set of events data as a whole contains the more intrusive communications data., including information on who has been in communication with whom, a person's location and internet connection records. Access to events data is authorised at a higher level within public authorities.
- Communications data that can be obtained from a CSP about an entity is limited to data held by a CSP in relation to the provision of a telecommunications service – it does not include data which may be held about a customer by a CSP more generally which are not related to the provision of a telecommunications service.
- The Bill provides that in the particular context of web browsing anything beyond data which identifies the telecommunication service concerned (e.g. bbc.co.uk) is content. Accordingly bbc.co.uk, google.co.uk or facebook.com would be communications data but data showing what articles has been read on the BBC website, what searches have been made on Google or whose profiles have been viewed on Facebook would be content and could only be acquired under a warrant.
- No authorisation is required for access to publically available information.

Examples of entity data	**Examples of events data**
Phone numbers or other identifiers linked to customer accounts; customer address provided to a communications service provider; IP address allocated to an individual by an internet access provider.	The fact that someone has sent or received an email, phone call, text or social media message; the location of a person when they made a mobile phone call or the Wi-Fi hotspot that their phone connected to; an internet connection record.

Investigatory Powers Bill

Related Communications Data/Equipment data

- Related communications data is data that may be obtained pursuant to an interception warrant. Where it is not necessary to acquire the entire content of a communication the warrant may be limited to the acquisition of related communications data including certain information extracted from the content.
- Equipment data is data that may be obtained under an equipment interference warrant.
- Related communications data and equipment data include communications data and any data which enables or otherwise facilitates the functioning of any system or service provided by the system. It also allows data with the characteristics of communications data to be extracted from the content of the communication where the data, once extracted, does not reveal the meaning of the content of the communication.
- Related communications data obtained under an interception warrant is equivalent to equipment data obtained pursuant to an equipment interference warrant.
- These definitions classify the types of data that may be obtained under both interception and equipment interference warrants. In particular, the defintions ensure that appropriate restrictions are applied to the selection for examination of data, regardless of the regime under which it has been acquired.
- All material obtained under interception and equipment interference warrants will be subject to the stringent handling safeguards set out in the Bill.
- These definitions make clear that it is only possible to extract certain data from the content of a communication under a warrant.

Examples of related communications data	**Examples of equipment data**
Data relating to any files attached to a message such as the date and time it was created and the author; any location information related to the communication, for example the location required to enable an application; any email addresses contained within a communication; download of an operating system and application updates.	The name of the person or account who stored a file on the device; the time and date that any files on the device were created or last modified; the operating system of the device and when it was last updated; the language settings on a device; the make or model of the device.

Content

- The content of a communication or other item of private information is the data which reveals anything of what might be reasonably be expected to be the meaning of that data, disregarding any meaning that can be inferred from the fact of the communication or the existence of an item of private information.
- Interception of the content of a communication is an offence except where provided for under the bill

Examples of content of a communication	**Examples of content of an item of private data**
The subject line and body an email; the audio/visual of a call; the content and title of attachments to an email; the body of a message on an internet messaging service.	A photograph; the title and content of a word document or spreadsheet ; a diary.