

INVESTIGATORY POWERS BILL: DATA DEFINITIONS

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. These definitions do not reflect current or anticipate technological developments and does not recognise the category of data which under modern communications means, is neither communications data nor content.

The Bill updates the definition of communications data in respect of telecommunications systems, services and operators to provide for technologically neutral, modernised definitions. The Bill also creates, for the first time, a definition of the content of a communication. New definitions of systems data and identifying data mean that all data that can be acquired under the Bill is consistently classified and is subject to appropriate safeguards, regardless of the power under which it was acquired.

The New Data Framework

For the purposes of the Bill communications may comprise two broad categories of data; systems data and content:

- Systems data enables systems to function and provide their services. It includes, but is not limited to, communications data. In relation to a communication, communications data is the subset of systems data which is necessary for the telecommunication system to transmit the communication.
- The content of a communication is the data which reveals anything of what might be reasonably be expected to be the meaning (if any) of that communication, disregarding any meaning that can be inferred from the fact of the communication.

Communications data can also include data that is held by a Communications Service Providers (CSPs) or available directly from the network which identifies a person or device on the network, describes how a person has been using a service or is about the architecture of the telecommunication system itself. Communications data 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.

When permitted by the Bill, certain data may also be separated from the remainder of a communication or from an item of information in circumstances where, if it were so separated, it would not reveal anything of the meaning (if any) of the communication. This information, which may be used to identify for example any person, event and their location, is identifying data.

Access to the data

Content, systems data and identifying data can only be acquired through the targeted and bulk interception and targeted and bulk equipment interference regimes. Accordingly acquisition of this information must be approved by a Judicial Commissioner through the double lock. Systems data and identifying data obtained under an interception warrant is classed as secondary data. Systems data and identifying data obtained via an equipment interference warrant is classed as equipment data. An interception or equipment interference warrant can be limited to the acquisition of just secondary or equipment data.

Targeted acquisition of communications data can be authorised by a designated senior officer within a public authority. The authorisation regime to obtain communications data reflects 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 which are not related to the provision of a telecommunications service e.g. political interests.

Examples

Content of a communication	
The subject line and body of 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	
Communications data	
Entity 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.	Events data 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.
Systems data (other than communications data)	
Messages sent between items of network infrastructure to enable the system to manage the flow of communications Router configurations or firewall configurations Software operating system (version) The period of time a router has been active on a network	
Identifying data (other than systems data)	
The location of a meeting in a calendar appointment Photograph information - such as the time/date and location it was taken Contact 'mailto' addresses within a webpage	