INVESTIGATORY POWERS BILL: COMMUNICATIONS DATA

What is it?

Communications data is information about communications: the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was written or said. It includes information such as the subscriber to a telephone service. Law enforcement, the security and intelligence agencies and other specified public authorities may acquire this data from communications service providers (CSPs). CSPs may also be required to retain it.

Why do we need it?

Communications data is an essential tool for the full range of law enforcement activity and national security investigations. Requests may be made for data in order to identify the location of a missing person or to establish a link (through call records) between a suspect and a victim. It is used to investigate crime, keep children safe, support or disprove alibis and tie a suspect to a particular crime scene, among many other things. Sometimes communications data is the only way to identify offenders, particularly where offences are committed online, such as child sexual exploitation or fraud.

What happens now?

When necessary and proportionate, CSPs can be required to keep certain types of communications data for up to 12 months under the Data Retention and Investigatory Powers Act 2014 (DRIPA). Law enforcement and the security and intelligence agencies may acquire that data and any other communications data held by CSPs for business purposes under RIPA. Requests must be for a specific statutory purpose. Other than in exceptional circumstances, they must be independently authorised. Safeguards are set out in two statutory codes of practice. The Government keeps the number of public bodies which can acquire communications data under constant review; only organisations which can demonstrate a continuing and compelling need are provided with the power. Police requests that are intended to identify journalists' sources must be authorised by a judge. Local authorities can only apply for communications data for the purpose of the prevention and detection of crime and local authorities' applications must be approved by a magistrate.

What will happen in the future?

The Investigatory Powers Bill will create a new statutory basis for the retention and acquisition of communications data. The Bill will enhance the safeguards that apply to communications data acquisition, building on the recommendations made by David Anderson QC. The Bill will close the growing capability gap that limits the ability of law enforcement to identify the sender of online communications or the internet services being used by a suspect or a missing person (see following section on Internet Connection Records).

What safeguards will there be?

Authorisations will have to set out why accessing the communications data in question is necessary in a specific investigation for a particular statutory purpose, and how it is proportionate to what is sought to be achieved. All authorisations will go through a Single Point of Contact (SPoC). The SPoC's role is to ensure effective co-operation between law enforcement bodies, the security and intelligence agencies, other specified public authorities and communications service providers and to facilitate lawful acquisition of communications data. They also play a quality control role, ensuring that applications meet the required standards.

Once it has gone through the SPoC, the application must be authorised by a Designated Senior Officer (DSO), who is independent of the investigation for which the communications data is needed. The Bill will provide a power that can ensure public authorities which access communications data infrequently will have to go through a shared SPoC (for example, by making use of the SPoC function within the National Anti-Fraud Network, as recommended by David Anderson QC). This will help to ensure that all applications are consistent and of sufficient quality.

The IPC will oversee how all law enforcement and the security and intelligence agencies use these powers. The Commissioner will audit how the authorities use them and report publicly on what they find.

What are the key provisions in the Bill?

- **Communications data retention and acquisition powers will be brought within a single, clear piece of legislation**

- **Other powers for acquiring communications data, such as those in the Health and Safety at Work Act 1974, will be repealed**

- **A new criminal offence of knowingly or recklessly acquiring communications data will be provided for as a firm check against abuse**

- **Bodies that make a small number of communications data requests can be required to share Single Points of Contact (SPoCs) to ensure requests meet accepted and consistent standards**

- **The definitions of communications data have been reviewed and are being updated to reflect changes in the way people communicate**

- **Communications Service Providers can only be required to retain communications data, including internet connection records, when served with a notice requiring them to do so. Access to this information will be limited, targeted and strictly controlled**