Communications Data

COMMUNICATIONS DATA is best known as the who, where, when, what and how of our internet activity and telephone calls. It differs from content which is seen as the most personal aspect of our communication. Because technology is so complex one definition is never completely accurate. The Investigatory Powers Act is littered with a number of different terms for communications data, each more complicated than the other. The Act makes it difficult to understand what the Government defined as communications data and content.

* *

What is communications data?

You create data whenever you send a letter, email or text, whenever you make a phone call, use the internet, use a connected device or use an app. This data was formerly split into two categories:

Communications data: the, who, when, where and how of any communication.

Content data: the detail of the message. The Act describes it as "the meaning" of a communication.

These terms were understandable but not 100% precise.

The Act attempts to offer new definitions for communications data, they attempt to acknowledge that in a connected world, everything we do and every device we engage with creates data.

* *

What other definitions are there?

The Investigatory Powers Act uses the following terms as examples of communications data. None of them offer one failsafe definition and distinction between communications data and content data, many of them are too complicated to explain clearly.

- Entity data: Information which identifies you. For example subscriber data, phone number, email address, postal address, IP address, type of device used. This is the, who and how of communications data.
- Events data: The where and when of calls, texts, emails, social media messages. This will include internet connection records.
- Systems data: Data which enables the system to work, i.e. your message to be sent or call to be made. Systems data is described as "communications data" and "other data" in the Bill.
- Identifying data: Communications data which is embedded into the content of a communication but because it is not defined as content can be looked at as communication data, for example when you send a calendar link as part of the content of an email.
- Secondary data: A term used to describe both systems data and identifying data when it has been gathered through interception.
- Equipment data: A term used to describe systems data and identifying data when it has been gathered through equipment interference.

Communications Data

Who can access communications data?

Under the Investigatory Powers Act the following bodies can gain access to communications data with a warrant signed by either a designated senior official within the organisation, or in the case of local authorities with a warrant signed by a magistrate.

- Police and National Crime Agency (NCA)
- Intelligence agencies: MI5, MI6 and GCHQ
- HM Revenue and Customs (HMRC)
- Department of Transport
- Department for Work and Pensions
- Serious Fraud Office
- The Scottish and Welsh Ambulance Service Boards
- Local councils
- National Health Service (NHS)
- The Ministry of Defence
- Department of Health
- Ministry of Justice
- Competition and Markets Authority
- Criminal Cases Review Commission
- Food Standards Agency

Communications data is the only part of the Investigatory Powers Act which is not subject to Ministerial authorisation or Judicial Commissioner review and approval.

Judicial Commissioners are asked to approve warrant requests for material relating to journalistic sources only.

* *

What is the Request Filter?

There is very little known detail about the Request Filter.

In David Anderson QC's review of bulk powers it was revealed that the Request Filter has not been fully developed or even designed.

All we know about the Request Filter is:

- It is a system which will be built by a private company.
- It will be operated by the Home Office on behalf of the Home Secretary.
- The Request Filter will act as a middle man between the public authorities and the communications providers.
- A targeted communications data authorisation will be needed to use the Request Filter.
- We do not know who will build the Filter or how much it will cost.
- Without further information it could be assumed that the Request Filter could become a "honeypot" of communications data.

* *

Don´t forget

- Whenever you make a call, send a text, send an email or go online you create communications data.
- Your communications data can reveal a very detailed trail of your online life.
- Telecommunication operators are now required to keep all our communications data for 12 months.
- The police, the tax man, the NHS and local councils can request access to your communications data.

Investigatory
Powers Act
Factsheet

BIG
BROTHER
WATCH