Investigatory Powers Bill

Key points

- Communications data (CD) is the context, but not the content of a communication: who was communicating, when, from where, and with whom. For example it can be a person's mobile phone number or email addresses used to send and receive emails, but it is not what is said in a telephone conversations or written in an email.
- Communications service providers retain some communications data under existing law, but data relating to the use of internet services is often unavailable. That includes data about what communications services a suspect or victim was using. Without new legislation, crimes enabled by email and the internet will increasingly go undetected and unpunished, and law enforcement agencies will find it more and more difficult to locate vulnerable people at risk of harm.
- The Investigatory Powers Bill will create provisions for UK Communications Service Providers (CSPs) to retain the data that law enforcement and the security and intelligence agencies need to investigate crime and safeguard national security in the digital age.

Background

- The Investigatory Powers Bill builds on the recommendations made by David Anderson QC, in his report, A Question of Trust as well as recommendations made by RUSI, the Intelligence and Security Committee of Parliament and the Joint Committee which considered the draft Communications Data Bill in 2012.
- Communications data is generally acquired from a service provider that retains that information. They may do so for business purposes, but they may also do so to comply with a data retention notice issued by the Secretary of State.
- Currently, communications service providers can be obliged under a data retention notice to retain certain types of communications data for up to twelve months, under the provisions of the Data Retention and Investigatory Powers Act 2014. The Bill will also require communications service providers to retain internet connection records. ICRs do not provide a full internet browsing history. The ICRs do not reveal every web page that a person visited or any action carried out on that web page. Local authorities will be prohibited from acquiring internet connection records.

Key facts

- Communications data is the 'who', 'when', 'where' and 'how' of a communication. It does not include the content of a communication.
- Communications data has played a significant role in every Security Service counter terrorism operation over the last decade.
- It is used in 95% of serious and organised crime investigations handled by the Crown Prosecution Service.
- Communications data has also played a significant role in the investigation of a large number of serious and widely reported crimes, including the Oxford and Rochdale child grooming cases, murder of Holly Wells and Jessica Chapman, and 2007 Glasgow Airport terror attack.

Quotes

"Communications data is still overwhelmingly the most powerful tool available to those investigating child sexual exploitation and identifying and safeguarding its victims and potential victims."
Keith Bristow, Director General, National Crime Agency

"It is regularly used to tackle criminals whose activities affect the wider community, such as repeat burglars, robbers and drugs dealers. Put simply, the police need access to this information to keep up with the criminals who bring so much harm to victims and our society."
Sir Bernard Hogan-Howe, Commissioner, Metropolitan Police

"For cases such as counter-terrorism, organised crime and large-scale fraud, I would go as far to say that communications data is so important that any reduction in capability would create a real risk to future prosecutions."
Keir Starmer MP, (former) Director of Public Prosecutions

Investigatory Powers Bill

Why do we need it?

- CD is essential for the investigation of cyber-crime and the protection of children online, where it is often the only investigative lead that will identify offenders.
- As the way we communicate changes, the data needed by the police is no longer always available.
- While data is available for traditional forms of communication, such as telephony, it is not always held for internet communications because CSPs do not retain all the relevant data.
- This means that while the police can identify all of the phone numbers called by a missing person before their disappearance, they are unable to tell what apps or social media services that person was using to communicate. This is an increasing problem for law enforcement.

What is new that the Bill will do?

- Provide for the retention by CSPs of internet connection records – a record of the internet services a device has connected to.
- Modernise the definitions of what constitutes CD to reflect both current and anticipated technological developments.
- Create a new criminal offence applying to persons in public authorities who unlawfully acquire communications data.
- Make clear the circumstances where CSPs can notify their customers that a request for their data has been made
- Provide judicial authorisation for requests by public authorities acquiring communications data to identify or confirm a journalistic source.

What are the safeguards?

- Only public authorities approved by Parliament can use the powers.
- Communications data can only be obtained on a case by case basis and must be authorised by a senior officer at a rank stipulated by Parliament.
- Only CSPs served with a data retention notice will be required to retain specified types of CD.
- The maximum period for that data to be retained by CSPs will be 12 months.
- The Information Commissioner oversees the compliance of security requirements for retained data by CSPs and its destruction at the end of the retention period.
- Independent oversight of CD powers will be provided by the Investigatory Powers Commissioner. As with its predecessor, the Interception of Communications Commissioner's Office, the IPC will audit public authorities' compliance with CD acquisition powers and produce reports that will be made publicly available on an annual basis.
- Providing a clear legislative requirement for judicial authorisation to be sought for CD requests where the intention is to identify or confirm a journalistic source.
- Local authority acquisition of communications data requires the approval of a magistrate and local authorities will not be able to acquire Iinternet connection records for any purpose.
- Any individual who thinks that the powers have been used against them unlawfully can complain to the Investigatory Powers Tribunal.
- A detailed statutory code of practice will set out the practices that must be followed by CSPs retaining data under a notice and public authorities who acquire the data.

Who can do it? When? Under what authorities?

The Bill will specify on the face of legislation which public authorities have access to communications data, as approved by Parliament, and only where there is a robust business case for them to do so The statutory purposes for which CD can be acquired other than for crime and national security include: public health, public safety, to collect taxes, to prevent death or injury in an emergency, investigate miscarriages of justice, trying to identify someone who has died to find next of kin, and for financial regulation.