Data Retention and Investigatory Powers Bill

Top Lines

- Communications data (CD) is the context, but not the content of a communication: who was communicating, when, how, from where, and with whom.
- Law enforcement and the intelligence and security agencies use this data to investigate crimes, bring offenders to justice and to save lives.
- On 8 April 2014, the European Court of Justice (ECJ) declared the EU Data Retention Directive (DRD) invalid. We must ensure that communications service providers (CSPs) continue to retain communications data in the future. If they do not, it will not be available to the police when they need it for an investigation.
- This legislation will ensure a clear basis in domestic law for the retention of communications data in the UK. It will, in practice, maintain the status quo, while also responding to the ECJ judgment.
- This Bill does not replicate the proposals from the Draft Communications Data Bill, published in 2012.
- The Bill is compatible with the ECHR and will contain the normal statement to this effect from the Home Secretary.

For information relating to other investigatory powers please see the separate factsheet.

What is Communications Data?

- Communications data is the who, when, where and how of a communication, but not its content.
- The police use it to prove or disprove alibis, identify associations between suspects, and tie an individual to a particular location or crime scene.
- Communications data has played a significant role in every Security Service counter terrorism operation over the last decade.
- It is regularly used in court: notably, in 95% of serious and organised crime investigations handled by the CPS.
- It has also played a significant role in the investigation of a very 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.
- Communications data will often be the only investigative lead. If this data is not retained, these cases will go unsolved.

Why do we need to legislate?

- Communications data is held by companies for their own business purposes (usually three months) and where mandated to do so in law.
- It can then be accessed by the police under the Regulation of Investigatory Powers Act 2000 (RIPA), where it is necessary and proportionate to do so for a specific investigation, subject to stringent safeguards.
- On 8 April, the ECJ declared the EU Data Retention Directive (DRD) invalid. Although the UK's own Data Retention Regulations remain in force, we need a clear legal basis for mandatory data retention in UK law.
- Otherwise, companies may soon start deleting data that is essential for law enforcement and national security.
- This legislation will mirror the provisions of the existing Data Retention Regulations, and create a clear basis in domestic law for the retention of communications data.
- It will also make changes to the regime to respond to elements of the ECJ judgment.

What do law enforcement need?

- Senior officers are clear that, without the data currently being retained under law, crucial investigations will become impossible. The data types in question are listed in a Schedule to the draft regulations published alongside the Bill.
- These are identical to the existing Regulations and include items like names, addresses, telephone numbers, dates and times of messages, device (i.e. phone or computer) identifiers and cell location information.

What about the Draft Communications Data Bill?

- This Bill does not replicate the proposals from the Draft Communications Data Bill.
- There remains a pressing need to update legislation to ensure that data for new types of internet communication are available in the future, as data for telephony has been in the past. The Joint Committee on the Draft Communications Data Bill accepted this requirement, subject to the appropriate safeguards.
- The Prime Minister has been clear that we will need to return to these issues in the next Parliament.

"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."
Sir Keir Starmer, (former) Director of Public Prosecutions

Data Retention and Investigatory Powers Bill

How are we responding to the ECJ judgment?

- The ECJ struck down the European Data Retention Directive, not our own laws. The judgment upheld the principle that data could be retained at the request of government, but found that the Directive itself lacked proper safeguards.
- It did not consider the robust safeguards that already exist in the UK's communications data regime. We believe that our internationally-respected retention and access regime already addresses most of the ECJ's criticisms.
- The Bill is compatible with the ECHR and will contain the normal statement to this effect from the Home Secretary.
- However, in order to respond to elements of the judgment and to ensure the Bill is compliant with ECHR, we are extending the existing safeguards in a number of ways. Many of these changes are set out in the regulations that accompany the Bill rather than on the face of the Bill itself:
  - Ministers will need to consider necessity and proportionality before issuing retention notices, as well as the impact of the notice on the provider.
  - There will be a maximum, rather than absolute, retention period of 12 months – data may be retained for less if it is not necessary or proportionate to keep it for longer.
  - There will be a clear requirement for the Secretary of State to keep notices under review.
  - Data retention notices will, as at present, be limited to a strict list of data types. This will be identical to the existing list in the 2009 Data Retention Regulations.
  - The content of the new notices will be far more specific e.g. setting out the data categories and services this retention applies to.
  - Access to data retained under this Bill will be limited to requests under RIPA and court orders.
  - Data security requirements will be set out in notices requiring a CSP to retain data, and will be enforceable.
  - The Information Commissioner's duties will be clarified, so that he oversees all relevant aspects of data retention.
  - We will create a Code of Practice on Data Retention, putting best-practice guidance on a statutory footing.
  - We will amend the data acquisition Code of Practice, ensuring (i) where there may be concerns relating to professions that handle privileged information (e.g. lawyers or journalists), law enforcement should give additional consideration of the level of intrusion; and (ii) making it clearer that the officer authorising access to data should be independent of the investigation.

What safeguards control access to communications data?

- RIPA provides for an ECHR-compliant regime governing the access to communications data. Specifically:
  - Data may only be acquired by public bodies that have been approved by Parliament to do so, and for specific statutory purposes (prevention/detection crime, national security, preventing death or injury etc.).
  - Data is obtained on a case by case basis and must be authorised by a senior officer (who is independent from the investigation) at a rank stipulated by Parliament. That authorising officer may only authorise a request for communications data if the tests of necessity and proportionality are met.
  - The full authorisations process is shown in the **diagram below**. The Joint Committee on the Draft CD Bill concluded that this was the '*right model*'.
  - Local authorities' requests for communications data must also be approved by a magistrate.
  - The Interception of Communications Commissioner provides independent oversight of the acquisition of communications data by public authorities. He conducts robust inspections and publishes an annual report.
  - The Information Commissioner oversees the processing and security of personal information held by CSPs, including communications data.