Data Retention and Investigatory Powers Bill

Government Note on the European Court of Justice Judgment

Communications data is used to piece together the activities of suspects, victims and vulnerable people: it proves and disproves alibis, it identifies links between potential criminals, it ties suspects and victims to a crime scene and helps locate vulnerable people at risk of imminent harm.

The recent judgment of the European Court of Justice which struck down the Data Retention Directive explicitly recognised the importance of data retention in preventing and detecting crime. This Bill is essential to ensuring that this crucial data is available to law enforcement in the future as it has been in the past and unless companies are required to retain that data, much of it would no longer be available.

Although the Court criticised elements of the Directive, it did not consider the robust safeguards that already exist in the UK's communications data regime. The Government has considered the judgment in detail to ensure that we get our response right on this crucial issue.

We believe that our internationally-respected retention and access regime already addresses many of the ECJ's criticisms. In order to respond to elements of the judgment and to ensure the Bill is compliant with the ECHR, however, we are extending the existing safeguards in a number of ways.

On 12 July Parliamentarians were sent a joint briefing on the Bill by Liberty, Privacy International, Open Rights Group, Article 19, Big Brother Watch and English PEN. Based on their analysis of the detailed judgment this briefing stated that any legislation mandating data retention by a Member State of the EU must comply with ten principles which were contained in the judgment.

This note outlines the Government's response to each of the 10 points contained in their briefing.

1. Restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and / or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences

- Given that it is impossible to predict in advance what data would need to be retained, this approach relies on data being retained only after a crime has been committed and/or an investigation has begun. Preservation only works if the data is there to preserve, and is of limited benefit without an existing retention scheme.
- There have been a number of reports published by the EU commission showing the value of communications data, and why "data preservation" is not a viable alternative. These include examples of where investigations could not be pursued because of the absence of communications data.

- In a Europe-wide investigation into online child sexual exploitation, of 371 suspects identified in the UK, 240 cases were investigated and 121 arrests or convictions were possible. Of 377 suspects in Germany, only 7 could be investigated and no arrests were made.
- The legislation will enable the Secretary of State to issue data retention notices to Communications Service Providers on a selective basis – only if she considers the obligation to be necessary and proportionate, for one of the authorised purposes. We will also add a requirement to keep notices under review
- We will ensure that specific details must be specified in the notice served on providers including the categories of data to be retained

2. Provide exceptions for persons whose communications are subject to an obligation of professional secrecy

- We will amend the data acquisition Code of Practice, ensuring that 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.

3. Distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned

- The legislation will limit any data retention to a strict list of data types specified in the Data Retention Regulations.
- We will ensure that specific details must be specified in the notice served on providers including the categories of data to be retained.
- It will enable the Secretary of State to issue data retention notices to Communications Service Providers on a selective basis – only if she considers the obligation to be necessary and proportionate.

4. Ensure retention periods are limited to that which is 'strictly necessary'

- The legislation will provide that data can be retained for a maximum period set out in the Regulations, which can be no longer than 12 months. Data will be retained for shorter periods if it is appropriate in any given case.
- The UK's 12 month retention period was put in place following a survey conducted by the Association of Chief Police Officers in 2005. That survey showed that it was necessary for the police to have access to data up to 12 months old.
- Further surveys in 2010 and 2012 reinforced the evidence base for this decision.

5. Empower an independent administrative or judicial body to make decisions regarding access to the data on the basis of what is strictly necessary

- The UK system of authorisation for access to data is by a senior individual from the organisation requesting data at a rank required by Parliament.
- Our access system was examined in detail by the Joint Committee on the Draft Communications Data Bill and they were satisfied that "*the current internal authorisation procedure is the right model*".
- A senior EU Commission official observed on a recent visit to the UK that he thought our access and oversight arrangements were the best in Europe. This notwithstanding,
    - We will take steps to enhance the independence of the authorising officer from the specific investigation for which CD is required through the relevant statutory Code of Practice.
    - To ensure that data can only be accessed where suitable safeguards are in place, the legislation will limit access to data retained under the legislation to RIPA, court orders and certain other limited circumstances specified in the regulations.

6. Restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes

- The Data Retention Directive was specifically required retention of data for purposes related to serious crime. The Bill ensures that data can be retained for a range of purposes which are the same purposes for which data can be accessed under RIPA.
- UK investigation of serious crime often requires the investigation of lower level individuals for activities that are not considered serious crime in order to build cases against higher ranked criminals.
- Such investigations would be severely hampered if data was retained only where it was linked to serious crime.
- However, the legislation will specify that data may only be retained if it is necessary and proportionate to do so.

7. Limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary

- 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.).
- Further restrictions ensure that bodies can only access the data that is necessary, for example local authorities cannot access traffic data, the most intrusive category of communications data.
- The UK system of authorisation for access to data is by a senior individual from the organisation requesting data at a rank required by Parliament.

- We will be taking steps to reduce the number of bodies who are able to access communications data.

8. Ensure the data is kept securely with sufficient safeguards to secure effective protection against the risk of abuse and unlawful access

9. Ensure destruction of the data when it is no longer required

- The UK imposes a number of security measures that go further than the requirements that were contained in the Directive.
- The legislation will ensure that these measures are formally made part of the data retention requirements placed on providers.
- The legislation will also clarify the duties of the Information Commissioner to audit communication provider compliance with the requirements for the security, integrity and deletion of the data.

10. Ensure the data is kept within the EU

- The notices to providers that require them to store data will specify the requirements for the storage of data. This may include restrictions on the location of retained data.
- Any data retention will be subject to the requirements in the Data Protection Act 1998. Data Protection Principle 8 provides that personal data should only be processed outside the EU if appropriate controls are in place.