The EU Data Retention Directive 2006/24/EC

Costs - £50 million over 8 years (Home Office)

Talking Points

Privacy

The government can apply, through the security services, to obtain details about individual communications. This is a negative impact on individual civil liberties. For the government to access confidential communications between private individuals is a breach of individual privacy.

Security of individual information

The government lost 25 million pieces of HMRC data. What safeguards are there to ensure the government – with similar safety precautions – cannot let our private communications data fall into the hands of third parties who wouldn't have access to it in the first place. After the loss of so much private data, a responsible government would refuse the opportunity to collect so much individual data.

A wide number of bodies are able to obtain private data

Out-law.com has found that the bodies that can access data under the directive include the Post Office, health authorities and local authorities. Therefore unaccountable bodies can access private data, a clear breach of privacy without any democratic redress by the voters. Councils have been heavily criticised for abusing the Regulations of Investigatory Powers Act to spy on families taking their children to school (Poole Council).

What is it?

A directive compelling all internet service and telecommunications providers to store all communication information from customers for a whole year. The directive aims to harmonise member states provisions relating to data retention for the uses of investigation and prosecution.

Under the directive, details of every phone call, email and text message will be saved by communications providers. While the content of the data will not be recorded, the time, identity of individuals and location of the communication will be recorded.

All data will be available to authorities already able to access information under the Regulatory of Investigatory Powers Act (councils, health authorities and even the Post Office).

Only through a court order will security services and police be able to access recorded data. The directive orders member states to establish or designate a public authority to administer data retrieval. Governments are also to set up suitable punishments for misusing data available under the directive.

Third Party Opinions

"*Mandatory data retention will place all the communications of everyone under surveillance.*" Tony Bunyan, Editor of Statewatch.

"Data retention can support the protection of individual rights only in few and generally less important cases. A permanent, negative effect on crime levels is not to be expected... [With data retention in place] citizens constantly need to fear that their communications data may at some point lead to false incrimination or governmental or private abuse of the data. Because of this, traffic data retention endangers open communication in the whole of society." The Open Rights Group.

"Where the government prevents the effective protection of personal data because of its appetite for surveillance, it opens up the gates for misuse of the data by third parties. Innumerable facts about the private life of prominent members of the public could be obtained by analysing traffic data. In the event of unauthorised access to retained traffic data, politicians could be forced to resign and officials could be blackmailed." Open Democracy.