Data Retention

DATA RETENTION is a key part of the Investigatory Powers Act. Data retention is when our internet, telephone, mobile and postal communications are kept by our telecommunications company for a year. The police, intelligence agencies, local authorities or government departments such as HMRC or the NHS can access the data.

What data is being retained?

Communications data: the who, when, where and how of your calls, texts, emails or internet connections. For more information please see our Communications Data Factsheet.

Internet connection records are a log of every website you visit and app you use. They detail the date, time, IP address and device you are using. Information about the other devices you are communicating with or connecting to is also retained. For more information please see our Internet Connection Records Factsheet.

Who holds this data?

Data is held by any person or organisation which the Act defines as a Telecommunications Operator.

Telecommunications Operator is an enormously broad term which includes any person, system or provider of communications for example:

- Any internet based service
- Email service
- App
- Cloud provider
- Wi-Fi provider
- Mobile phone operator
- Postal service
- Coffee shops and cafes
- Hotels
- Public Wi-Fi
- Pubs, bars and restaurants
- Public transport/airports
- Health devices/wearables
- Cars

Is encryption impacted?

Yes, the Government are worried about there being any "safe spaces" online. Because encryption prevents anyone other than the sender and intended receiver being able to read the content, the intelligence agencies, police and Government are unable to read any communication which has been encrypted.

The Act has made it lawful for the Government to demand that any business remove "electronic protection" which has been applied to any communications or data if it is "technically feasible" for the business to do so.

A Technical Capability Notice can be used by the Home Office to request a company build a backdoor into their systems so encrypted communications can be accessed by the intelligence agencies.

This approach contradicts the general consensus that encryption is needed to keep people, business, organisations, governments and the national infrastructure safe and secure.

Data Retention

What is a Technical Capability Notice?

The Investigatory Powers Act allows the Home Secretary to serve a Technical Capability Notice on a Telecommunications Operator, this means:

- A company must hold customers data for 12 months in a secure system.
- If needed a new system must be built for the data to be held in.
- The system built will be subject to analysis, oversight and modification by the National Technical Assistance Centre (NTAC); a part of the Home Office.
- Data may be added to a Request Filter system.
- The Request Filter will be a new system built by a private company for the Home Office.

Alternatively the Home Secretary can issue a National Security Notice. A company with more than 10,000 users has to adhere to what the notice says and hand over any requested data or information when asked. This can include access to data or communications which have been encrypted.

Will all operators have to comply?

Yes. Operators have to do what the notice orders. If they don't they can have a civil case brought against them.

This is not a new practice. Section 94 of the Telecommunications Act 1984 made it legal for any telephone company to hand over data on UK citizens.

Section 94 was used on all UK citizens to monitor our telephone activity post 9/11.

Are warrants needed to access the data?

- Data retention notices must be reviewed and approved by a Judicial Commissioner.
- Companies subject to a notice can request a review, which will be carried out by the Secretary of State who will be required to seek advice from the Investigatory Powers Commissioner.
- Companies subject to a notice can request a review, which will be carried out by the Secretary of State who will be required to seek advice from the Investigatory Powers Commissioner.
- A Secretary of State will sign off on all data retention warrants, be it a National Security Notice or a Technical Capability Notice.

Don't forget

- A Telecommunications Operator either in the UK or abroad has to hold their customers communications data for 12 months.
- The operator may be required to build a new system to hold internet connection records.
- The Government can monitor the systems built by the private companies.
- Data retention for 12 months of all people suspected of criminal behaviour or not, is considered a breach of our human rights and a breach to our right to a private life.

Investigatory Powers Act Factsheet | BIG BROTHER WATCH