

# Internet Connection Records

**INTERNET CONNECTION RECORDS (ICRs)** list all our internet activity. Every website we visit and every smart phone app we access. ICRs are an intrusive record of our lives based on what we do and when we go online. Under the Investigatory Powers Act every Telecommunications Operator is now required by law to hold this information for a year. These records will be accessible to the police, intelligence agencies and other organisations including HMRC and the NHS.

\*\*\*\*\*

## What are Internet Connection Records?

**When you visit** a website you usually start at the websites homepage such as [www.bigbrotherwatch.org.uk/](http://www.bigbrotherwatch.org.uk/). The Act defines this part of a website address (the part before the first forward slash) as communications data which is considered to be non-intrusive information.

**When you explore** the rest of the website such as [www.bigbrotherwatch.org.uk/factsheets](http://www.bigbrotherwatch.org.uk/factsheets), the address has information after the forward slash, the Act defines this as content, information which is considered to be intrusive.

**Separating out** this information and making sure no content is collected may be very difficult and expensive for companies to do because sometimes the address will contain content information regardless of where the forward slash is.

**Your ICR will** include customer account information, detail of the device being used, IP address, the date and time of browsing, how much data is downloaded or shared, who you are connecting with and what devices you connect to.

\*\*\*\*\*

## Why are ICRs intrusive?

**Our online searches** can reveal more about us than we realise. They can reveal our health and finances, our sexuality, race, religion, age, location, family, friends and work connections. They can also reveal our internal thoughts, anxieties and desires, information we won't even share with the people we trust the most.

**Our basic browsing history** is considered to be personal information.

**As the Internet of Things** takes hold and more of our lives are connected to mobile or internet devices we will be creating even more connection records than can be imagined. The government, police and intelligence agencies now have access to all this information.

\*\*\*\*\*

## Do other countries collect ICRs?

**No other European** or Commonwealth country require Telecommunication Services to store this data.

**Australia** recently introduced a data retention law but explicitly stated that web logs of a user's browsing history should not be kept due to the intrusive nature of the data they hold.

**Denmark** scrapped a similar scheme after seven years because it was proven to be useless to law enforcement work.

# Internet Connection Records

## Who can request access to an ICR?

**Internet Connection Records** can be accessed by a large number of organisations and government agencies. The complete list is:

- Police and National Crime Agency (NCA)
- Intelligence agencies: MI5, MI6 and GCHQ
- HM Revenue and Customs (HMRC)
- Department of Transport
- Department for Work and Pensions
- Serious Fraud Office
- The Scottish and Welsh Ambulance Service Boards
- Local councils
- National Health Service (NHS)
- The Ministry of Defence
- Department of Health
- Ministry of Justice
- Competition and Markets Authority
- Criminal Cases Review Commission
- Food Standards Agency

**Local authorities** and council officials will not be permitted access to this data.

\*\*\*\*\*

## How will ICRs be held?

**Data Retention Notices** will be issued to a Telecommunications Operator. These will insist that the company retains Internet Connection Records of all their customers.

**Telecommunications Operators** are the companies you purchase your internet connection, Wi-Fi and mobile telephone services from.

**These companies** will be required to create systems to hold the data securely. These systems will be overseen by the Home Office.

**Companies** will also have to seek approval from the Home Office if they wish to create new products, services or rebrand their business.

**The cost** of these systems will be covered in part, by the Government. This means that taxpayers' money will be used to build these surveillance systems.

\*\*\*\*\*

## Don't forget

- Telecommunication Operators are now required by law to keep a log of all of our online activity for 12 months.
- Every website you visit, the time, location and information about your device is stored.
- The police, intelligence agencies and other organisations including HMRC and the NHS must produce a warrant to access Internet Connection Records.
- Special secure systems will be built by private companies to hold the data. These systems will be overseen by the Home Office.