Investigatory Powers Bill

Key points

- Internet connection records (ICRs) are records of the internet services that have been accessed by a device. They would include, for example, a record of the fact that a smartphone had accessed a particular social media website at a particular time.
- The draft Bill will require that ICRs are retained by communications service providers. It will limit access to ICRs for one of three purposes:
    - To identify the sender of a communication. This could be used to locate the particular device from which an illegal image was uploaded to a website at a particular time. At the moment, this is not always possible. This can be a significant problem for child sexual exploitation investigations.
    - To identify the communications services a person is using. This would allow the police to determine whether a missing person was using a particular smartphone app or social media website prior to his or her disappearance. Today, that information is frequently not available, leaving law enforcement agencies with no investigative avenues.
    - To determine whether a person has been accessing or making available illegal material online. This is a valuable tool in child sexual exploitation investigations in the course of which it may otherwise be impossible to prove that a suspect has been accessing illegal content online.
- ICRs do not provide a full internet browsing history. The ICRs do not reveal every web page that a person visited or any action carried out on that web page.

Background

- The Bill will enable us to require providers to collect and retain internet connection records, allowing law enforcement agencies to attribute illegal activity on the internet to a person in the real world.
- Without this data, it is not always possible to attribute a particular action on the internet to an individual person. Examples for the use of ICRs include:
    - if a server hosting child abuse images was seized, Internet Connection Records when used with Internet Protocol (IP) resolution data would allow law enforcement agencies to trace the individuals who accessed the images where the server holds a log of the IP addresses and the times they were used.
    - identifying how a criminal gang are communicating online
- A data retention notice can require a CSP to retain this data for up to 12 months.

Key facts

- Of 6025 cases relating to the sharing of child abuse imagery, referred to CEOP Command of the NCA, 862 (14%) would require the retention of ICRs to have any prospect of identifying a suspected paedophile.
- Of 600 serious criminal suspects covered by an interception warrant, more than 300 were accessing online communications services. These services would currently be invisible to law enforcement through historic CD requests:
    - 81% were accessing a specific social media service;
    - 73% were using a specific instant messaging service; and
    - 41% were accessing a particular email website

Figures from Ofcom on the way people communicate:

- 66% of adults in the UK now own a Smartphone and 81% of them use it to send emails.
- Video internet telephony calls are used by 18% of Smartphone users;
- A substantial proportion of Smartphone users also use their device to make online transactions:
    - 45% for making online purchases
    - 44% for online banking; and
- 62% of Smartphone users have a social media application downloaded on their device.

Investigatory Powers Bill

Why do we need it?

- Evidence indicates that the majority of criminal suspects are using online communications services, and other online services of potential investigative value, that are currently invisible to communications data requests. Ofcom statistics also show that the trend towards online communications is only increasing. For example:
  - The proportion of consumers in the UK using internet telephony services tripled from 12%-35% between 2009 and 2014.
  - 19 billion online instant messages were sent in 2012, compared to 17.6 billion text messages.
- ICRs can be crucial for:
  - Identifying the sender of an online communication (often involving IP address resolution)
  - Identifying which communication services a person has been using
  - Identifying where a person has accessed illegal content

What are ICRs?

- Internet connection records are records captured by the network access provider (e.g. the Internet Service Provider or Wi-Fi operator) of the internet services with which a uniquely identifiable device (e.g. a laptop or mobile phone) interacts.
- It will involve retention of a destination IP address but can also include a service name (e.g. Facebook or Google) or a web address (e.g. www.facebook.com or www.google.com) along with a time/date.
- It could never contain a full web address as under the law these would be defined as content.
- You may be able to see that a person has used, google.co.uk or facebook.com but you would not be able to see what searches have been made on google or whose profiles had been viewed on Facebook.

Who can do it? When? Under what authorities?

- A data retention notice for internet connection can be placed on a CSP by the Secretary of State, where necessary and proportionate.
- Relevant public authorities can then acquire the data for one of three purposes, where necessary and proportionate, on a case by case basis.
- Local authorities will be prohibited from acquiring internet connection records for any purpose.

What are the safeguards?

- The Bill stipulates the statutory purposes for which this data can be accessed and CSPs can only be required to retain the data where the Secretary of State considers it necessary and proportionate to do so for those purposes.
- A designated senior person can only approve applications where the intent is to determine:
  - which individual has used a specific internet service
  - how a subject of interest is communicating online
  - whether an individual is accessing or making available illegal material
- Local authority access to internet connection records is prohibited so that they will never be able to request a list of internet services accessed by an individual
- Where the intent is to determine other internet services accessed, the application must be rejected
- This retention of this data will be subject to stringent security requirements, including audit by the Information Commissioner.
- Each application to access this data has to be made individually, with an explanation of why each element of the statutory requirements is fulfilled.
- Each application is scrutinised by an appropriate manager who considers the proportionality of the individual application.
- The public authorities legally permitted to request data will be subject to inspection by the Investigatory Powers Commissioner, which is independent from Government and will report an annual basis.
- The Investigatory Powers Commissioner will audit CSP disclosure systems.

What is new?

- The Counter Terrorism and Security Act 2015 provided for the retention of certain data to resolve IP addresses. However, without the retention of ICRs, resolving an IP address back to a single user will often not be possible as multiple users may be associated with that IP address. ICRs therefore provide the unique identifier to distinguish between different users of a shared IP address.
- ICRs will also be able to be used to determine how subjects of interests are communicating and whether they are accessing illegal material.