INVESTIGATORY POWERS BILL: INTERNET CONNECTION RECORDS

What are they?

An internet connection record (ICR) is a record, comprised of a number of items of communications data, of an event about the service to which a customer has connected to on the internet, such as a website or instant messaging application. It is captured by the company providing access to the internet. Where available, this data may be acquired from communications service providers (CSPs) by law enforcement and the security and intelligence agencies.

An ICR is not a person's full internet browsing history. It is a record of the services that they have connected to, which can provide vital investigative leads. It would not reveal every web page that they visit or anything that they do on a web page.

Why do we need them?

ICRs are vital to law enforcement investigations in a number of ways. For example:

- To assist in identifying who has sent a known communication online, which often involves a process referred to as internet protocol (IP) address resolution

- To establish what services a known suspect or victim has used to communicate online, allowing investigators to request more specific communications data

- To establish whether a known suspect has been involved in online criminality, for example sharing indecent images of children, accessing terrorist material or fraud

- To identify services a suspect has accessed which could help in an investigation including, for example, mapping services

What happens now?

There is no current requirement in law for CSPs to keep ICRs and this information may therefore be unavailable to law enforcement agencies, meaning that often they can only paint a fragmented intelligence picture of a known suspect. Internet protocol (IP) address resolution identifies the sender of online communications. This is assisted by the Counter-Terrorism and Security Act 2015 (CTSA), but it is only possible in a limited range of cases. Because CSPs will often allocate the same IP address to many devices on their networks, it is often difficult for them to identify, in response to a request by law enforcement, which particular user or device uploaded an illegal image to a file sharing website. This is a significant problem for law enforcement. For example:

From a sample of 6025 referrals to the Child Exploitation and Online Protection Command (CEOP) of the NCA, 862 (14%) could not be progressed and would require the ICR provisions in the Investigatory Powers Bill to have any prospect of being progressed.

That is a minimum of 862 suspected paedophiles, involved in the distribution of indecent imagery of children, who cannot be identified or potentially prosecuted without this legislation.

This also means that in some cases law enforcement do not have access to essential data regarding an investigation as it has not been retained – this includes, for example, the identity of an individual suspected of sharing indecent images of children or the people with whom a missing person was last in contact.

What will happen in the future?

Communication service providers can be required to keep ICRs for a maximum period of 12 months. This will be invaluable to law enforcement for the prevention and detection of crime and protecting national security. The Bill will build on the provisions in the CTSA that provide for the resolution of IP addresses. Bringing the powers together in one place will ensure openness and that safeguards are applied consistently.

What safeguards will there be?

Applications to acquire ICRs will only be approved using the stringent application process for communications data requests and only for a limited set of specified purposes and subject to strict controls. Local authorities will be prohibited from acquiring ICRs for any purpose.