Operational Case for the Retention of Internet Connection Records

Contents

1 – Key Facts

Definitions:

- Communications data (CD) – the who, where, when and how of a communication but not its content – is a vital tool used to investigate crime and protect the public. It is used in 95% of serious and organised crime prosecution cases handled by the Crown Prosecution Service Organised Crime Division and has been used in every major Security Service counter-terrorism investigation over the last decade.

- Internet Connection Records (ICRs) are a type of CD. They are a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet.

- ICRs do not provide a full internet browsing history. They do not include details of every web page visited or anything done on that web page.

The Value of ICRs:

- The draft Bill would enable the retention of ICRs by communications service providers, to be used by law enforcement in three ways:
    1. to identify the device that has sent a communication online;
    2. to identify the communications services a device has accessed; and
    3. to identify the accessing of illegal online services or websites
- Under the provisions in the draft Bill, local authorities will not be able to access ICRs.

The Problem:

- As ICRs are not currently retained, law enforcement capabilities are degrading due to rapid technological change and because more and more communications are taking place online:
    - 66% of adults in the UK now own a Smartphone and 81% of them use it to send emails;
    - The proportion of consumers in the UK using internet telephony services **tripled from 12%-35%** between 2009 and 2014; and
    - **19 billion online instant messages** were sent in 2012, compared to 17.6 billion text messages

- Without ICR retention, it remains impossible for law enforcement to identify consistently who has sent a particular communication online.

- Referrals from the National Centre for Missing and Exploited Children (NCMEC) report instances where child abuse images have been uploaded and shared via social networking and email services. The National Crime Agency (NCA) receives around **1300 to 1500 referrals a month** from NCMEC compared with around 1200 a year ago, and under 400 in 2010.

- One NCMEC referral can contain as many as **100** to **5000** indecent images of children linked to a single account. **One referral can also contain**

thousands of IP addresses that could relate to a single offender or victim using multiple devices, or multiple suspects and victims.

- Analysis of a sample set of **6025** NCMEC referrals made to the Child Exploitation and Online Protection Command (CEOP) of the NCA shows that:
    - **862 (14%)** would require the retention of ICRs to have any prospect of identifying one or more suspected paedophiles.
    - There were a further **3470 (58%)** cases where, although an IP address could be resolved to a fixed line account that may help identify an individual suspect, ICRs could help identify additional devices and accounts, which may lead to the identification of multiple other suspects.
- That is a minimum of 862 suspected paedophiles, involved in the distribution of indecent imagery of children, who cannot be identified under existing legislation.

- Examples from the Metropolitan Police and NCA show the impact of not being able to identify an individual device from a communication online, including:
    - A case where an individual started a sexualised conversation online with a 13 year old girl but could not be identified.
    - An investigation into the sharing of indecent images of children where the perpetrator could not be identified.
    - A fraud investigation where it was known that suspects were transferring fraudulently obtained money online with mobile phones but the specific devices used could not be established.

- A review of ongoing and historic cases by the Metropolitan Police Service (MPS) and NCA also shows that without ICR retention, and as technology continues to change, law enforcement agencies can frequently only establish a fragmented intelligence picture of how a known suspect has communicated.

- Analysis of the use of mobile devices by approximately 600 serious criminal suspects demonstrates that more than 300 were accessing online communications services. These services would currently be invisible to historic CD requests and were only identified in these cases because an interception warrant was in place, which would not be available in the majority of law enforcement investigations:
    - **81%** were accessing a specific social media service;
    - **73%** were using a specific instant messaging service; and
    - **41%** were accessing a particular email website

- If an investigator cannot establish what communications services a suspect or victim has used online, they will not be able to make additional requests for CD to those companies in order to ascertain who someone has been communicating with.

- Even if it is suspected that certain services or websites are being used, based on their popularity with the public, it is unlikely to be necessary and proportionate to approach such companies on the off-chance that a suspect or victim has accessed their services.

- ICRs would enable law enforcement to approach an individual provider to acquire CD where it is known that a specific device has accessed their service online.

- Case studies provided by the Metropolitan Police and NCA demonstrate the damage caused where CD cannot be used to establish what online communications services have been used by a known suspect, including:
    - A fraud case with potential financial losses of tens of millions of pounds where it has not been possible to establish the extent of the criminal network.
    - An operation into an organised crime group involved in human trafficking where the full extent of the group cannot be established.
    - An investigation into the distribution of indecent imagery of children where CD could not identify how members of a criminal network were communicating and only thanks to the seizure of devices was it possible to identify more than 250 additional suspects.

2 – What is an ICR?

Internet Connection Records (ICRs) are a type of communications data (CD). CD is information about who was communicating, when, from where, how and with whom; the context but not the content of a communication. For example, CD for mobile phones might be billing and location information and for online communications, the internet protocol (IP) addresses (explained below) identifying the individual, or at least the device, that sent an email or posted a message on the internet. CD is used in the investigation and prosecution of a broad range of crimes. It enables the police to build a picture of the activities, contacts and whereabouts of suspects and victims. It can also be used to identify and locate vulnerable people. It can be used in evidence and has been used in 95% of serious organised crime prosecution cases handled by the Crown Prosecution Service Organised Crime Division.

Specifically, an ICR is a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet. ICRs comprise a very narrow set of data, such as numerical internet protocol (IP) addresses and port numbers – which may be used to establish that a particular device accessed a particular internet service or website – as well as details of the time that a specific service was accessed.

For example:

Peter is a member of an organised crime group involved in drugs trafficking. Yesterday at 3pm he used his Smartphone to log on to his mobile network and access the internet, with the intention of emailing his drugs supplier to organise a delivery of cocaine. To access the internet at all, Peter's phone needed to borrow an address from the UK mobile network company, enabling it to receive communications from the internet. This is a numerical address known as an internet protocol (IP) address (there are a limited number of these and there is a central register of which people, organisations or companies control each one). Peter then used his Smartphone to visit an email website at two minutes past three. To do this, his phone used the IP address it had been allocated by the mobile network provider, 62.25.961.0, to send an electronic request to the IP address of the server of the email website. A server is a physical computer that acts as a host, providing a specific service to other devices over a network, in this case an email website over the internet. The email website servers are located at the IP address 216.239.321.10 and the server responded by sending a reply to Peter's phone (at 62.25.961.0), which Peter saw as the email website, also at two minutes past three. Having sent his email at four minutes past three, Peter disconnected his phone from the mobile network at five past and switched it off.

In this case a record processed by the mobile network provider of the internet service connected to by the IP address allocated to Peter's phone, at a certain point in time – is an internet connection record.

So a specific example of an ICR from this scenario might be "IP 62.25.961.0 connected to IP 216.239.321.10 at 15:02"

3 – The Value of ICRs

The draft Bill will provide for ICRs to be retained so that they can be used, where necessary and proportionate, in three ways to benefit law enforcement investigations:

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

2. To establish what services are being used by a known suspect or victim to communicate online, enabling further CD requests to be made to the providers of those online services e.g. to establish who the suspect or victim has been communicating with.

3. To establish whether a suspect has accessed illegal services online e.g. to access illegal terrorist material or for the purposes of sharing indecent imagery of children.

These three purposes focus on identifying suspects, victims and criminal activity; fundamental aspects of law enforcement investigations.

4 – Why is there a problem?

In a “traditional” telephony environment, a person had a landline or mobile phone, and the company providing the phone line or contract then kept records of what calls were made (for how long etc.) to enable the person to be billed.

This meant that in the past, if a law enforcement agency needed to acquire communications data, they were able to do so because it would be held by the landline or mobile phone company that was providing the communications service. However, this is no longer the case.

Today, the company providing a phone and phone line may not be the company through which someone communicates with their friends and contacts. For example, services like social media websites or instant messaging applications are not run by the network providers in the UK. Whilst these services use the phone line and the internet to route calls or send messages, they don’t use the traditional “voice” service that is offered by the UK phone network company. They are accessed through the internet, as “data”. So the UK network provider knows that someone has accessed the internet but they do not routinely hold details of what services on the internet have been accessed. This is what ICRs would show.

Companies such as social media websites and instant messaging applications may keep records of the calls or messages that have occurred, when these happened and who called whom. The police and other agencies can ask them today for CD – subject to the strict controls in the Regulation of Investigatory Powers Act 2000 – but this requires the police and agencies to know what services the person has been using. Without ICRs, law enforcement will not be able to identify that an individual device has connected to an online service such as a social media website and so will not know to approach that company for more information.

Under the current legal framework communications service providers in the UK can be served with a notice by the Secretary of State that requires them to retain certain types of communications data for up to twelve months. This ensures that the data can then be accessed historically by law enforcement agencies where necessary and proportionate and in relation to a specific investigation. However, ICRs cannot currently be retained under a retention notice.

Legislation does currently allow law enforcement to access internet connection records if they are held by the UK network provider. However, as ICRs cannot be retained under a retention notice, this means that law enforcement can usually only currently access ICRs on a forward-looking basis. They would not be able to access the data retrospectively, through what is often referred to as a “historic CD request”, unless a company happened to retain this information for their own business purposes. This is fundamental because law enforcement will often need to be able to access CD historically e.g. where a vulnerable child has gone missing and CD is needed to establish who they were communicating with before they disappeared.

5 – How does this problem relate to the three purposes for which ICRs can be accessed in the draft Bill?

Purpose 1 (identifying the individual device that has sent a communication online): the fact that ICRs are not retained causes significant problems because law enforcement know a specific communication has taken place online but cannot link this to an individual. As set out in the example given about Peter, there are only a limited number of IP addresses on the internet. This means that companies providing internet access will sometimes need to share IP addresses between a large number of different devices at the same time:

> When Peter used his Smartphone to access the internet with IP address 62.25.961.0 yesterday, 5,000 other customers from his mobile network were also using their phone to access the internet with this same IP address. When Peter's phone made a request to access an email website the website's server was still able to send the correct information back to Peter's phone, but only because of other identifying information sent with the communication. Such other identifiers include port numbers, which act as an extension to an IP address in the same way that four digit extension numbers work for the prefixed phone number of an individual office building. So because Peter was the only person at that time using IP address 62.25.961.0 on port 10007, the information from the email website's server is directed to his device (at 62.25.961.0:10007).

In circumstances where law enforcement need to establish who has sent a communication online but IP addresses are being shared, they will also need other identifiers to link the communication to an individual device.

The Counter Terrorism and Security Act (CTSA) was passed earlier this year and included provisions in relation to IP address resolution. These provisions were specifically to ensure that UK communications companies under a communications data retention notice can be required to retain additional identifiers, such as port numbers.

However, the provisions in the Counter Terrorism and Security Act do not enable the retention of ICRs. This means that it remains impossible to resolve IP addresses consistently because ICRs will often be needed to do so.

Using the example about Peter demonstrates why ICRs will often be crucial to resolve an IP address:

Peter has sent his email arranging the delivery of cocaine to his supplier. However, his supplier was known to the police and has now been arrested. As the supplier's phone was seized when he was arrested, the police are aware of Peter's email. Peter has set up his email account in false details and the supplier refuses to identify him. Assuming that the police have no prior intelligence about Peter, this email would now be their only investigative lead to identify him. Information attached to the email shows that it was sent by a device connected to the internet on IP address 62.25.961.0 yesterday at four minutes past three. As there is a central register of which people, organisations or companies control each IP address, the police know that 62.25.961.0 is controlled by a UK mobile network operator. They therefore make a communications data request to that company to establish what device was using IP address 62.25.961.0 at four minutes past three yesterday afternoon. The mobile network operator confirms that 5,000 of its customers were using that IP address at that time and so the police are unable to establish what device sent the communication. Under provisions in the Counter Terrorism and Security Act, the UK mobile network operator also retains information about what port number each of the 5,000 devices using IP address 62.25.961.0 was connected to at the relevant time. The police therefore make an additional CD request to the email company that Peter used to send his message to see if they hold corresponding information. However the email provider, which is an overseas company, does not hold data showing that the email was sent by a device connected to port 10007. It therefore remains impossible to establish which of the 5,000 devices sent the communication and the police cannot identify Peter as part of the investigation.

Communications data retention notices can only be placed on companies processing data in the UK. Where someone is using an internet service from an overseas company, in this case the email website, IP resolution will rely on that company happening to hold enough data to match the additional data that is retained by the UK internet access provider under the CTSA.

If ICRs were retained, this would have provided crucial additional information in the scenario above. Once the police had established the relevant UK mobile network operator, they could have asked them what device was using IP address 62.25.961.0 at four minutes past three yesterday afternoon, **to access the specific online communications service**. This would be likely to provide the UK mobile network operator with enough information to identify Peter's device as it is unlikely that many, if any, of the other 5,000 devices using that IP address were accessing that email website in the same minute as Peter.

Purposes 2 and 3 (establishing whether a known device has accessed communications services or illegal websites): the absence of ICR retention causes problems in these circumstances where there is a known suspect or victim but it cannot be established what services are used online.

In the example given about Peter:

> The police suspect that Peter is involved in the trafficking of class A drugs. They have wider intelligence that Peter contacted his supplier on his mobile phone yesterday afternoon to organise a delivery but have no other information to help identify the supplier. The police know the mobile network that Peter uses and, following stringent tests of necessity and proportionality, acquire CD from the mobile network provider to try and establish who Peter communicated with the previous afternoon. The only data returned from the network provider confirms that Peter accessed the internet through their network yesterday afternoon between three and five past. It is therefore inferred that Peter may have organised the criminal activity online but, because ICRs are not retained, it is not known what internet services he accessed and the police cannot therefore make further enquiries to establish who he contacted.

In this scenario, the fact that ICRs are not retained means that the police have no intelligence about who is supplying drugs to Peter and no other way of establishing their identity or the extent of Peter's criminal network.

6 – How big is the problem?

Rapid technological change means that law enforcement's inability to access online CD is significant and will only get worse if it continues to be impossible to require communications companies to retain ICRs.

More and more communications are taking place over the internet and as this happens it follows that an increasing proportion of CD will be unavailable when it is needed. In his recent report into investigatory powers the Independent Reviewer of Terrorism Legislation, David Anderson QC, gives examples demonstrating the speed with which technological developments are changing the way people communicate:

- in 2014 61% of adults owned a Smartphone, compared to 27% in 2011;
- 57% of people used a mobile phone to access the internet in 2014, compared to 28% in 2011;
- in 2012 19 billion messages a day were sent over online instant messaging applications compared to 17.6 billion text messages (and there are many more instant messaging applications now than there were in 2012);
- the proportion of consumers in the UK using internet telephony services almost tripled between 2009 and 2014, from 12%-35%[1]

The Ofcom Communications Market Report for 2015 also includes details of the changing way in which people are communicating as technology develops:

- 81% of Smartphone users use their device to send emails;
- Video internet telephony calls are used by 18% of Smartphone users;
- 62% of Smartphone users have a social media application downloaded on their device;
- 72% of adults who go online have a social media profile, compared to 22% in 2007;
- 23% of internet users were regular users of internet telephony services as at March 2015; and
- In contrast to the increasing use of online services, the number of text messages being sent is falling. Mobile contract customers sent 171 mobile messages per month in 2014, which is a decrease of 10.2% from the previous year, equating to 19 messages per month.[2]

Ofcom considers the reasons for the decline in the use of text messages and concludes that: "The most likely reason behind the declining average monthly mobile messages is increasing Smartphone take up and use of alternative communication methods, such as email, instant messaging and the messaging services provided by handset makers and social networking sites."[3]

[1] "A Question of Trust: Report of the Investigatory Powers Review" David Anderson QC, pg 50, paras 4.6-4.8
[2] "Ofcom: The Communication Market Report, published 6th August 2015"
[3] "Ofcom: The Communications Market Report, published 6th August 2015" Ofcom, pg 294"

These trends in the way people communicate are indicative of the potential scale of the problem that is being caused because ICRs are not retained. However, this is not evidence in itself of the specific problems that law enforcement currently face.

7 – What is the evidence to show that ICR retention is needed?

Law enforcement have provided clear evidence that the retention of ICRs is necessary in order for them to progress their investigations and, therefore, protect the public.

Purpose 1 (identifying the individual device that has sent a communication online): For the reasons set out earlier in this paper, ICRs will often be crucial in identifying a device from a specific communication online. In such cases communications data will often be the only investigative lead, such as where the police receive a referral containing one or more IP addresses used to share indecent imagery of children. If it is not possible to identify an individual device in these circumstances, the case will be dropped since CD is the only intelligence held and the identity of the individual, or individuals, who has shared these images cannot be confirmed.

Referrals from the National Centre for Missing and Exploited Children (NCMEC) report instances where child abuse images have been uploaded and shared via social networking and email services. The NCA receives around **1300** to **1500** referrals a month from NCMEC compared with around **1200** a year ago, and under **400** in 2010.

One NCMEC referral can contain as many as **100** to **5000** indecent images of children linked to a single account. **One referral can also contain thousands of IP addresses** that could relate to a single offender or victim using multiple devices, or multiple suspects and victims. For example, login details will sometimes be shared amongst groups of offenders to create a 'library' of child sex abuse. Online sharing sites enable groups of offenders to login and trade child abuse images and live-stream abuse.

A study into the ability of law enforcement to investigate referrals made by NCMEC found that of 6025 referrals over a nine month period, one third are unresolvable meaning that evidence of child abuse cannot be investigated further. However half of these unresolvable cases, or 14% (862 referrals) of the total sample set, could be investigated if ICRs were retained.

A full breakdown of the 6025 cases is as follows:

- **862 referrals (14%)** could only be taken further if ICRs were retained. In the absence of ICR retention, there is no way to progress these cases. As one referral can contain multiple IP addresses relating to multiple individuals, that is a minimum of 862 suspected paedophiles that could not be identified in just nine months.

- **178 cases (3%)** are potentially resolvable under existing law because law enforcement may have been provided enough additional information by the online service provider to do so. However, in all of these cases, ICRs would provide an additional identifier that would help to identify an individual account or device.

- In **948 cases (16%)** it would not be possible to identify who had sent the online communication, even with the retention of ICRs. This is for a number of reasons, such as no IP address being provided by the online service provider, the use of online anonymisation techniques, or because the relevant online communications had taken place over a year ago; which is beyond the period that CD can be retained by UK communications companies under a data retention notice. Improvements in the amount of data and timeliness of referrals provided by communications companies in these cases would improve law enforcement's capability to investigate referrals but a portion are likely to remain impossible to progress.

- **4037 cases (67%)** contained at least one fixed IP address relating to a communication sent within the last twelve months. This is an IP address that is not being shared by multiple subscribers at the same time, such as where someone is using a fixed line broadband account to access the internet. This means that in these cases, it may be possible to identify an individual from the referral.

- However, as set out above, one referral can contain many IP addresses relating to multiple accounts, suspects or victims. Of the 4037 referrals that contained at least one fixed IP address, **3470 (58% of the total sample set)** also contained at least one shared IP address, likely to relate to an individual's mobile phone or other mobile device, such as a tablet computer. If ICRs were retained, law enforcement would be able to try and resolve these additional IP addresses, which could in turn identify additional suspects, or additional accounts and devices used by a single suspect. This means that ICRs would be of significant value in progressing these referrals, providing crucial additional investigative leads that would otherwise be unavailable.

It is also important to note that identifying an individual from an online communication is often only the first step in an investigation and ICRs may also be crucial in progressing it further. For example, in this sample set there are 862 referrals where ICRs would be the only way of identifying an individual account. If ICRs were retained and law enforcement were able to identify suspects from these referrals, they would then look to build further intelligence e.g. to establish how this suspect has been communicating, in order to identify further suspects or victims. If a suspect is communicating online, then retained ICRs might be the only way to do this. For this reason, the purposes for which the draft Bill will make ICRs available must not be considered in isolation. While the first stage of an investigation may be to identify a suspect from a communication online (purpose 1), the next step may be to identify how they have been communicating and whether they have been accessing wider illegal websites (purposes 2 and 3).

In summary:

Of 6025 cases referred to CEOP, 862 (14%) would require the retention of ICRs to have any prospect of identifying a suspected paedophile, or group of paedophiles, accessing indecent imagery.

There were a further 3470 (58%) referrals where, although at least one IP address could be resolved to a fixed line account that may help identify an individual suspect, the same referral could contain thousands of other shared IP addresses for which ICRs would help identify additional devices and accounts, which may lead to the identification of multiple other suspects.

Specific case studies demonstrating the impact on investigations where IP addresses cannot be resolved are set out at **ANNEX A**.

Purposes 2 and 3 (establishing how a known device has accessed communications services and illegal websites): analysis of the use of mobile devices in relation to approximately 600 suspects in serious crime investigations shows the prevalence of the use of online communications services by these individuals.

In 50% of these cases, over 300, the use of online services was detected (in the remaining cases, the absence of online services detected is typically because no devices enabled to access mobile data have been targeted). The use of online services could only be identified in these cases because interception warrants were in place.

The interception of communications content can only be authorised in very limited circumstances and for only three statutory purposes; the prevention and detection of serious crime, in the interests of national security and for the economic well-being of the UK where there is a direct link to national security. In addition, there are only a very limited number of intercepting agencies. These are: MI5, the Secret Intelligence Service, the Government Communications Headquarters (GCHQ), the National Crime Agency (NCA), the Metropolitan Police Service (MPS), the Police Service of Northern Ireland, Police Scotland, HM Revenue and Customs and the Ministry of Defence.

Due to the very limited circumstances in which the interception of communications content can be authorised, this technique cannot be used in most law enforcement cases, including the majority of criminal investigations and all non-crime cases such as certain missing persons investigations. This means that in most cases, investigators will be reliant instead on other investigative techniques, particularly CD, to establish what services an individual has used to communicate. However, without ICR retention, it will not be possible to use communications data to establish how someone has communicated online, even where investigators know the identity of the suspect and the device being used. The table below shows the prevalence of the use of specific communications services among the 300 plus cases where online services were detected from an interception warrant.

Communications service	% of cases service detected
Social Media Service A	81%
Instant Messaging Service A	73%
Social Media Service B	48%
Email Service A	41%
Email Service B	17%
Online Telephony Service A	16%
Instant Messaging Service B	14%
Email Service C	10%

Had these cases not met the extremely high threshold for the use of interception, the data would not be available. Those data show: that in 81% of cases a suspect was using a specific social media service, that 73% of the suspects were using a specific instant messaging service, and that in 41% of cases a suspect was accessing a particular email provider. These figures clearly demonstrate that without an interception warrant and without ICRs, investigators will regularly only be able to use CD to establish a fragmented and incomplete picture of the services that a suspect has been using to communicate (**Case Studies 7-11**, at **ANNEX B**, demonstrate the damage being caused to law enforcement investigations because it is not possible to establish what communications services suspects have been using online).

In addition to these 300 plus cases, the Metropolitan Police Service has provided further evidence in relation to 27 seized mobile phones to establish the most prevalent communications applications (apps) installed on these devices. Data from the devices demonstrates again the prevalence of the use of online communications apps by criminal suspects, including a number of the same services detected on the 300 plus cases considered above.

Communications Application	% of cases service detected
Instant Messaging Service A	63%
Social Media Service A	41%
Online Telephony Service A	22%
Social Media Service B	22%
Instant Messaging Service B	22%

In the case of these 27 devices, had they not been seized, it would not have been possible to establish from CD requests all of the services that had been used to communicate. For example, it would not have been known that almost two thirds of the devices had been used at particular times to access a specific instant messaging service or that one fifth of the devices had accessed a specific online telephony service.

While seizing a device is often crucial and can be used to establish more information about how a suspect has communicated, it will not always be the preferred course of action in an investigation, as it is an overt action that will normally involve an arrest. For example, in the early stages of an investigation into an organised crime group, investigators will want to develop intelligence on the group covertly, which will often involve making CD requests to establish previous linkages between group members. Currently, investigators will not know whether they have been able to establish such linkages fully because they will not know whether the group members are communicating online (**Case Study 10**, at **ANNEX B**, provides an example of a case where investigators were forced to make an arrest and seize a device earlier than they intended because they could not use CD to establish how suspects were communicating).

Given the popularity of certain online services with the public at large, such as some social media or email websites, law enforcement may be able to infer that a suspect or victim has been using a certain online communications service. However, communications data can only be acquired subject to rigorous tests of necessity and proportionality. Approaching a range of popular online service providers on the off-

chance that a suspect or victim has accessed their services is unlikely to meet this test. In addition, there will be no guarantee that a suspect or victim does use such services so this approach would often return no results. In addition, such an approach would also not capture the use of smaller websites or applications, so the use of such services could still not be established. ICRs would enable law enforcement to approach an individual provider to acquire communications data where it is known that a specific device has accessed their service online.

The impact of ICRs not being available to establish the online communications services being accessed by a specific device is clear. If an investigator cannot establish what communications services a suspect or victim has used, they will not be able to make additional requests for CD to those companies in order to ascertain who someone has been communicating with. This could mean that crucial intelligence and evidence is not available e.g. where a suspect has communicated with other members of a criminal network online. In light of the evidence provided by law enforcement, there are also likely to be very large numbers of cases where significant investigative opportunities have been missed and where the impact of this will never be known because the necessary data, ICRs, simply cannot be accessed.

8 – What will the Bill do?

The draft Bill would require, where necessary and proportionate, the retention of ICRs by UK communications companies that are under a data retention notice, for up to twelve months. Law enforcement would then be able to acquire them on a case-by-case basis, where it was necessary and proportionate to do so in the course of an individual investigation, in order to: identify what device had sent an online communication, establish what online communications services a known individual had accessed or identify whether a known individual had accessed illegal services online.

Under the provisions in the draft Bill, local authorities would be prohibited from accessing ICRs.

A number of frequently asked questions about ICRs are at **ANNEX C**.

9 – ANNEX A – Case studies for purpose 1

Case Study 1 – Metropolitan Police – Child sexual exploitation:
An individual engaged in a sexualised conversation with what he believed to be a 13 year old girl in a teenage chat room. The IP address he was using in the chat room was captured by the police. However, the communications service provider was unable to resolve this IP address to a single user due to IP address sharing. If internet connection records were retained it would be possible to ask the network provider, which of their customers had used the specific IP address to access the chat room at a given point in time. This would have provided critical intelligence to assist in identifying the suspect.
As it was not possible to resolve this IP address, the investigation could not be continued.

Case Study 2 – Metropolitan Police – Child sexual exploitation:
An individual stated in an internet chat room that he had a sexual interest in young children and had "touched" in the past. His profile in the chat room also included a number of images of young children. The chat room provided the police with the IP address used to send the messages. However, the mobile network provider was unable to resolve this IP address to an individual due to IP address sharing. If internet connection records were retained it would be possible to ask the network provider, which of their customers had used the specific IP address to access the chat room at a given point in time. This would have provided critical intelligence to assist in identifying the suspect.
As it was not possible to resolve this IP address, the investigation could not be continued.

Case Study 3 – Metropolitan Police – Child sexual exploitation:
Intelligence showed that an individual had accessed a shared file through a peer to peer network, containing indecent imagery of children. The IP address and time of connection was captured by the police. However, the communications service provider was unable to resolve this IP address to a single user due to IP address sharing. If internet connection records were retained it would be possible to ask the network provider, which of their customers had used the specific IP address to access the shared file at a given point in time. This would have provided critical intelligence to assist in identifying the suspect.
As it was not possible to resolve this IP address, the investigation could not be continued.

Case Study 4 – Metropolitan Police – Fraud:
This is an investigation following a referral from a bank, whose customers were being contacted by phone and persuaded to hand over passwords to their online accounts. Information provided by the bank (IP addresses) demonstrated that suspects were using mobile devices to transfer large amounts of money through online apps. However, the mobile network provider was unable to resolve many of these IP addresses to an individual because they were being shared by multiple users. If internet connection records were retained it would be possible to ask the mobile network provider, which of their customers had used the specific IP address to access the relevant banking app at a given point in time. This would have provided critical intelligence to assist in identifying the additional suspects.

This investigation is ongoing and it remains impossible to identify all potential suspects because of unresolvable IP addresses.

Case Study 5 – Metropolitan Police – Fraud:
This operation relates to a malware based fraud that is targeting an online currency service. Since the breach was identified, 480 customers have been affected with losses of £85,000 being redeemed to bank accounts in various countries, including the UK. Online apps have provided information (IP addresses) demonstrating that mobile devices were being used to transfer money online. However, the mobile network provider was unable to resolve some of these IP addresses to an individual because they were being shared by multiple users. If internet connection records were retained it would be possible to ask the mobile network provider, which of their customers had used the specific IP address to access the relevant online app at a given point in time. This would have provided critical intelligence to assist in identifying the additional suspects.
This investigation is ongoing and it remains impossible to identify all potential suspects because of unresolvable IP addresses.

Case Study 6 – Metropolitan Police – Fraud:
This is an investigation into a phishing attack against a film company in which the company owner's work email account was accessed and money was moved from the company's bank account. Online app providers have provided information (IP addresses) demonstrating that mobile devices were being used to transfer money online. However, the mobile network provider was unable to resolve some of these IP addresses to an individual because they were being shared by multiple users. If internet connection records were retained it would be possible to ask the mobile network provider, which of their customers had used the specific IP address to access the relevant online app at a given point in time. This would have provided critical intelligence to assist in identifying the additional suspects.
This investigation is ongoing and it remains impossible to identify all potential suspects because of unresolvable IP addresses.

10 – ANNEX B – Case studies for purposes 2 and 3

Case Study 7 – Metropolitan Police – Fraud:
This is an operation into a serious malware based fraud with potential financial losses standing at tens of millions of pounds. A predominant member of the organised crime group responsible has been identified as residing in the UK. It is known that this suspect has used an internet enabled device and intelligence indicates that he uses this device to communicate online with his overseas network. As internet connection records are not currently retained, it has not been possible to identify what online communications services this suspect has used through communications data requests. This means that investigators have not been able to identify wider suspects and cannot establish the full extent of his criminal network overseas, which could provide vital investigative leads.
This investigation is ongoing and the inability to access ICRs continues to hamper its progress, limiting investigative opportunities.

Case Study 8 – National Crime Agency – Human Trafficking:
This is an investigation into an organised crime group involved in drug smuggling, human trafficking and associated money laundering. Members of the group are known to have used multiple devices to communicate, including internet enabled devices. As internet connection records are not currently retained, it has not been possible to establish the extent of online communications services used by the group through CD requests and the true extent of the group cannot, therefore, be established. Investigators have no wider intelligence to show how the group are using the internet.
This investigation is ongoing and the inability to access ICRs continues to hamper its progress, limiting investigative opportunities.

Case Study 9 – National Crime Agency – Distribution of Indecent Imagery of Children:
On September 11th 2015, seven men were convicted of child sexual abuse offences and handed sentences totalling 107 years. His Honour Judge Lambert said during sentencing that this case was 'evil beyond rational understanding'.

This investigation related to an organised crime group which coordinated grooming and contact sexual abuse of extremely young infants, in addition to making and distributing Indecent Images of Children. The abuse was live-streamed using internet based communication services and the images were distributed using social media as well as the wider Internet.

The NCA gathered vital intelligence from numerous devices seized from 12 core suspects which showed frequent messaging via online communication services. This information enabled the investigation to be widened, further establishing 262 other paedophiles involved internationally, 38 of whom remain unidentified. Usage of these applications is not shown in traditional communication data records.

Had Internet Connection Records (ICRs) been retained by service providers, law enforcement may have been able to identify other participants without being wholly reliant on seizing devices.

In this case, access to retained ICRs would have provided vital intelligence to identify who these people were and in turn identify their communications and further establish links between suspects to enable enforcement action and safeguarding of victims.
This investigation was reliant on seizing suspects' devices to reveal the extent of communications between child abusers. Much of this information would have been available through CD if ICRs were retained. ICR retention would also enable the identification of 38 suspects currently unidentified and believed to be involved in contact sexual abuse and the sharing of indecent imagery of children.

Case Study 10 – National Crime Agency – Fraud:
This is an investigation into credit card fraud online. It was known that two email addresses were being used to set up customer accounts and purchase goods online with stolen credit card details. Through CD, these email addresses were traced to two individuals who were arrested in July 2013.

This provided further investigative leads in relation to other suspects. As the offences under investigation were being conducted exclusively online, establishing the use of online communications services to establish contacts between the additional suspects was crucial. However, as ICRs are not retained it was not possible to build intelligence of the use of such services through CD requests. This meant that investigators were forced to arrest the additional suspects and seize their devices and then build intelligence and evidence retrospectively. Since the initial arrests, a further 16 individuals have been arrested and charged with related offences. Significant additional intelligence has been provided by forensic analysis of the suspects' devices. This included confirming the use of multiple communications services that were invisible to CD requests.

However, even with the analysis of seized devices, the absence of ICR retention has caused significant difficulties for the investigation because it has not been possible to link known activity online related to the criminality with the seized devices, and therefore the suspects.

In addition, information provided by an email provider (IP addresses) has identified that an email address relevant to the criminality was being connected to with a mobile device (dongle) that has not been seized. From wider intelligence, it was also known that the organised crime group used such a device to connect to the internet.

However, the mobile network provider has been unable to resolve the IP addresses from the email provider and it is therefore impossible to prove the link between the email account and the suspects. The retention of ICRs would make it possible to attribute this online criminality to the relevant devices.
This is an ongoing investigation and the absence of ICRs continues to hamper its progress by making it impossible to attribute specific online activity to known suspects. The operation has been severely hampered as a result.

Case Study 11 – National Crime Agency – Drugs Trafficking:
This is a drugs trafficking investigation into an Albanian organised crime group. National Crime Agency Officers observed three suspects moving packages of drugs

in and out of a flat in London. The three individuals were arrested and when the flat was searched, more than £100,000 cash, several kilograms of class A drugs and a number of mobile phones were seized.

Analysis of these seized devices demonstrated that the suspects were communicating using a number of online services, including to pass coded messages to arrange the importation and distribution of drugs. The communications data obtained from these devices resulted directly in two of the suspects being charged with conspiracy to supply 500kgs of cocaine.

However, these three suspects are believed to represent only a small cell within a much larger organised crime group and gaps in intelligence remain because ICRs are not retained. Specifically, information from the devices held has identified another internet enabled phone relevant to the investigation that has not been seized. Without ICRs, it is not possible to establish what online communications services this device has accessed, which could provide crucial intelligence to identify wider members of the group.
The three suspects have been successfully prosecuted but the full extent of the organised crime group remains unknown because lines of enquiries have had to be ceased in the absence of ICR retention.

10 – ANNEX C – FAQs

Q. Is this about spying on peoples' internet browsing history?

- No, this data would not provide a full internet browsing history. ICRs do not include details of every web page visited or anything done on that web page.
- This is about helping law enforcement and the security agencies identify which uniquely identifiable device has been interacting with a specific internet service (such as a server holding illegal images) or which internet services such a device has been communicating with.

Q. Do you really need ICRs to tell you that a suspect or victim will use popular online services e.g. Facebook?

- Yes. Public authorities that can acquire communications data may only do so subject to rigorous tests of necessity and proportionality.
- Approaching a range of popular online service providers on the off-chance that a suspect or victim has accessed their services would not be likely to meet this test.
- ICRs will enable law enforcement to approach online service providers to acquire communications data where it is known that a specific device has accessed their service.

Q. Which public authorities will be able to access ICRs?

- Only public authorities approved by Parliament are able to acquire communications data.
- Under provisions in the draft Bill, local authorities will be prohibited from accessing ICRs.

Q. Do law enforcement agencies currently make request for ICRs?

- Currently, law enforcement are able to access ICRs where necessary and proportionate to do so in relation to a specific investigation.
- However, they will only be able to access this data on a forward-looking basis, or where a company happens to hold this information for their business purposes, because communications companies cannot be required to retain it.

Q. What are the safeguards for accessing ICRs?

- The acquisition of ICRs is subject to the same rigorous safeguards as any other CD request.
- This data can only be accessed by public authorities that have been approved by Parliament and, under the draft Bill, local authorities will not be able to access it.
- These public authorities can only access CD where it is necessary and proportionate to do so in relation to a specific investigation.

Q. Why was the retention of ICRs not included in the Counter Terrorism and Security Act?

- The scope of the provisions in the Act reflected the extent of cross-Government agreement in the last Parliament.
- The Act provided a step in the right direction. However, where IP addresses are being shared by multiple users, capabilities continue to decline because ICRs are not retained.
- Communications data retention notices can only be placed on companies

processing data in the UK. Where someone is using an internet service from an overseas company, such as an email website, IP resolution will rely on that company happening to hold enough data to match additional data that is retained by the UK internet access provider under the Counter Terrorism and Security Act. Such information will regularly not be provided.

- If ICRs were retained, this would provide crucial additional information in these circumstances. It would enable the law enforcement agency to ask the UK company that is under a retention notice what devices' IP address were connected to the email website at a particular point in time.
- This would be likely to provide the UK company with enough information to identify the relevant device.