Annex A - TECHNOLOGY AND THE IMPACT ON INVESTIGATIONS

The internet has revolutionised communications

The infrastructure over which communications are transmitted has fundamentally changed with the development, and increased use of the internet. In turn the devices and way in which we access and interact on the internet has changed.

When the Regulation of Investigatory Powers Act 2000 (RIPA) was written a mobile phone could only be used for phone calls and text message. Today we are able to access the entire internet from our phones and mobile devices which means we use them for many more things at home and on the move from; emailing, browsing the internet, online banking, location services, directions, social networking, reading and listening to music.

Our style of communication has also moved from person to person to social media, broadcasting messages to groups of people that are likely to have never met or ever intend to meet.

- In 2015 the average adult spends 2.5hrs a week online on the move (five times that of 2005).
- Instant messaging use has increased from 38% in 2013 to 42% in 2014 driven by services such as Facebook messenger and WhatsApp.
- Social media is used by 80% of internet users aged between 35 and 44 compared with 12% in 2007.

Increasingly, the use of 'traditional' communications is becoming outdated. Landline phone numbers are decreasing as people opt for more convenient methods of communication.

Impact of Internet based Communications on Investigations

The rapid change of global communications technology introduces a digital challenge to Law Enforcement.

The internet has transformed the way in which people communicate. The nature of the internet means that there are no borders and as such the use of the internet for crime is a global problem and ultimately needs a global solution. Individuals are able to contact people all over the world in milliseconds, for no additional cost on multiple platforms. This advantage also extends to criminal use where connections are made where they wouldn't have been before. It also means that services are provided to UK customers from all over the world. The services cited as the most used by internet users such as Microsoft, Google, Facebook etc are predominantly based in the US creating challenges between domestic and international legislation.

Whilst these services are legitimate they are frequently used by criminals to facilitate crime which was not foreseen in the creation of these capabilities and creates competing demands on these companies and their duty to shareholders and customers.

The internet facilitates actions of those wishing to cause harm to the public and provides a degree of anonymity in doing so. The internet enables crime to be carried out on an industrial scale from online fraud to the sharing and distribution of child abuse images. New criminal activities have also been created with the advent of the internet such as the hacking of personal data which is held to ransom.

Whilst criminals become more adept at using the internet to facilitate crime, the capability that Law Enforcement (LE) has under current legislation has degraded since it does not enable powers of investigation to keep pace with the change in technology.

The change in technology, how people interact on and connect to the internet has also affected what information and intelligence Law Enforcement Agencies (LEA) are able to gather in the course of investigations. With the correct and appropriate access to this information LEA would be able to improve profiling and understanding of a suspect or victims' movements, contacts and actions both proactively and reactively. Arguably, making investigations more efficient and timely.

Traditional and Digital Communications Data Explained

Traditional Communications Data

Traditionally, communications over landlines and mobile networks meant that Communication Service Providers (CSPs) kept records of who spoke to who, how, when and where they were. A large portion of this information would be found on an individual's phone bill.

Figure 1: Example of Communications Data held under RIPA 2000

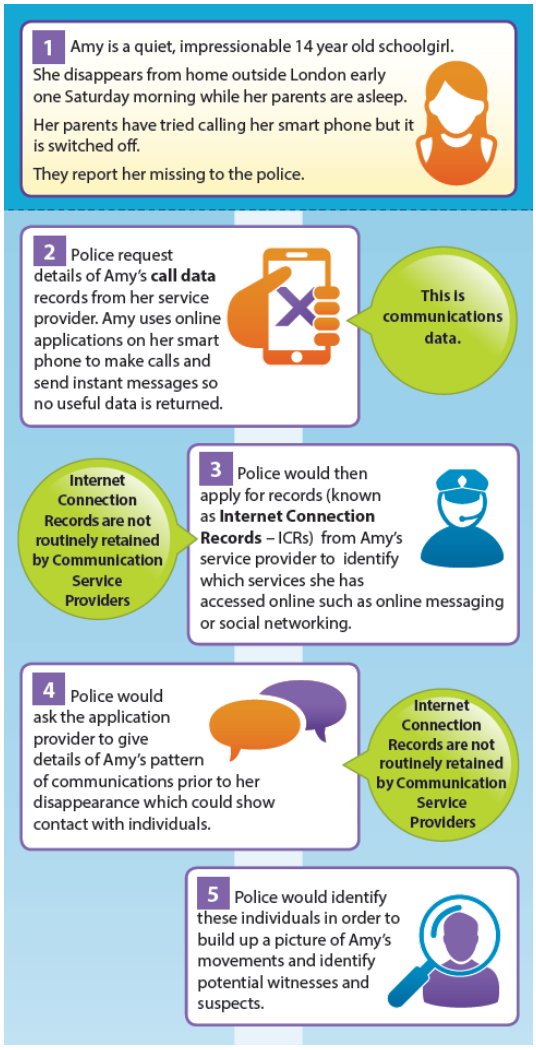
Date	Time	Type	Duration	A Party	B Party	IMEI	Site	Postcode	Last Cell
03-Oct-14	18:37:07	Mobile	00:00:44	7777111111	7787444444	3562870570	Hammersmith	W12 0HS	W12 0HS
03-Oct-14	18:52:10	Mobile	00:05:52	7777111111	7553662445	3562870570	Hammersmith	W12 0HS	W12 0HS
03-Oct-14	19:12:46	Mobile	00:01:19	7777111111	7787444444	3562870570	Hammersmith	W12 0HS	W12 0HS
03-Oct-14	20:22:35	Mobile	00:00:18	7777111111	7957776614	3562870570	Hammersmith	W12 0HS	W12 0HS

WHEN HOW WHO WHERE

This data is available to LEAs subject to RIPA 2000 authorisations and is still used in almost all cases by LEAs since it will often provide either a crucial starting point for an investigation or support leads of enquiry. RIPA means that UK CSPs have to retain details of their customers communications for 12 months, if it is not requested by LEAs within this time period it is automatically deleted.

A 12 month retention period is important because it is often unknown that a criminal act will take place. As such data must be stored proactively to allow for re-active investigations. (Further information on retention periods is available in **Annex E**.)

Figure 2: Use of Communications Data from 'traditional' communications



Digital Communications Data

Current legislation and access to this data has not kept pace with 21st Century capabilities and LEAs are increasingly blind to criminal communications and actions online.
Securing the equivalent of communications data online to that which is currently held offline takes LEA a step towards gaining back the ground that has been lost in the digital world between LE and criminal activity online, or facilitated by the internet.

Law Enforcement can not currently consistently access CD from online communications because not enough data is routinely stored by service providers. CSPs do not record the same type of information for online based communication as they do for traditional telephony. CSP business models are concerned with the amount of data their customers are using rather than the individual records of phone calls, texts and services accessed online. They retain data that is useful for billing, marketing and identifying trends of use across their customers rather than details of individual customer use.

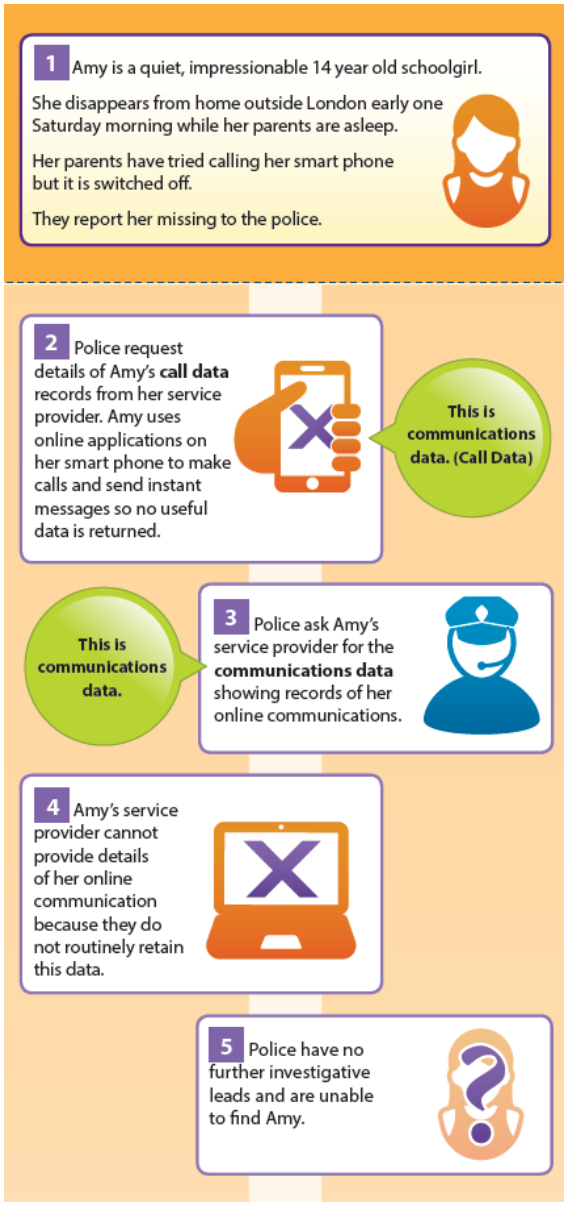
To maintain the LEAs' needs, the require to have better access to online CD, and current provisions do not meet the LE requirement to effectively investigate criminal activity when it is facilitated by online services.

Figure 3: Example of Communications Data held by CSPs for internet based communications

Date	Time	A	IP Address	Access point	Duration	Data upload	Data Download	IMEI	Site postcode	Bearer
03-Oct-14	18:37:07	7777111111	10.186.133.222	MobileTel	00:06:19	41705	230	3562870570	W12 0HS	3
03-Oct-14	18:52:10	7777111111	10.95.236.113	MobileTel	00:00:12	2182	7919	3562870570	W12 0HS	3
03-Oct-14	19:12:46	7777111111	10.58.134.140	MobileTel	00:06:31	1162	184	3562870570	W12 0HS	3
03-Oct-14	20:22:35	7777111111	10.42.165.73	MobileTel	00:07:48	6761	179800	3562870570	W12 0HS	3

WHEN WHERE

Figure 4: Example of the current capability to access online Communications Data



Improvements Law Enforcement need to online Communications Data

Internet Protocol Address Resolution (IPAR) is used to link an individual or account to an action online.

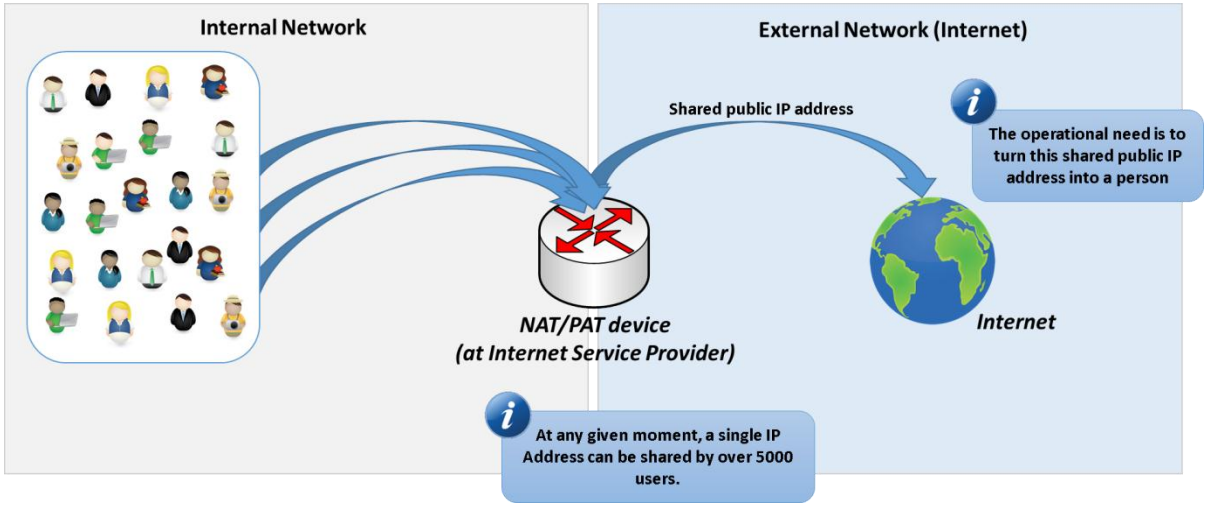
IPAR is increasingly challenging due to the amount of information that is passed over the internet and the Internet Protocol (IP) used to link devices / actions to individuals.

An IP address is the unique number assigned to every device on the internet. The IP address is akin to a phone number in traditional CD or a postal address that identifies where a letter is destined for.

The growth of the internet means that since the 1980s predications have been made that the original 4.3billion IPv4[1] addresses would be exhausted. This finally happened in 2011 and was mitigated to some extent by changes in the IP address allocation and routing infrastructure of the internet.

The process of NAT (Network Address Translation) and Port Address Translation (PAT) which enables service providers to manage the limited number of IP addresses available more efficiently makes IP Address Resolution (IPAR) difficult since IP addresses are shared. One 'public' IP can be used by many thousands of 'private' users making it impossible for an action online to be linked back to a specific device without further identifying information.

Figure 5: The NATPAT Problem



The problem of resolving IPs is exacerbated by the fact that servers across the world are not synchronised in terms of timestamp. An IP address with a date and timestamp to the tenth second captured for example by Facebook may be seconds out from the timestamp used by Vodafone in the UK whose service is used to access the site. To allow for this difference, search terms are widened by

[1] Internet Protocol version 4

a few seconds either side of the Facebook timestamp and as such the search term can return tens of thousands results.

The Counter Terrorism and Security Act 2015 (CTSA) intended to make it possible for LEAs to resolve IP addresses: engagement with CSPs and technology companies has identified that insufficient information is retained to enable IP addresses to be resolved in all situations, particularly on mobile internet access.

Without additional information about these communications over the internet, LEA are unable link a device to actions online and identify crucial information for investigations.

Annex B - BILL PROVISIONS FOR COMMUNICATIONS DATA

Internet Connection Records Explained

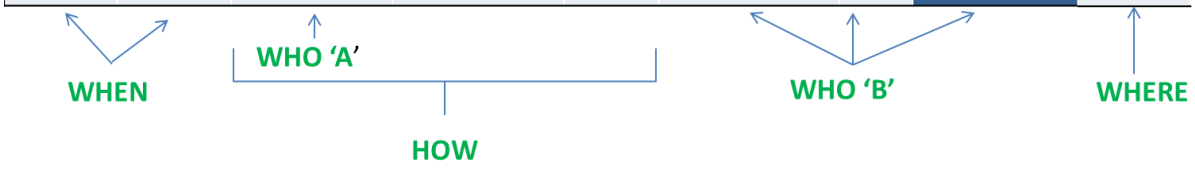
The Bill introduces Internet Connection Records (ICRs) as a term for the data which details the connections made from a device across the internet to other online services. These ICRs will record the following information:

1. The time of the connection – providing the **when**
2. The location of the device making the connection – providing the **where**
3. The service(s) the device was accessing – providing the **how** but **not what** was done on that service.
4. The identity of the device – that can lead to understanding the **who**

Yet to be defined, the additional data an ICR could include port numbers, destination IP addresses, time and service or host name.

Figure 6: Example of what an Internet Connection Record could look like

Date	Time	MSISDN	Source IP	Source Port	Dest. IP	Dest .Port	Service / Domain	Post Code
07/10/15	09:17:26	07771966917	234:96:17:113	2237	141.92.130.226	443	Lloyds Bank	W12 0HS
07/10/15	09:18:37	07771966917	234:96:17:107	61123	213.174.196.17	80	Easyjet	W12 0HS
07/10/15	09:19:15	07771966917	234:96:17:119	8987	238.226.19.35	5222	WhatsApp	W12 0HS
07/10/15	09:19:55	07771966917	234:96:17:119	1592	50.31.0.12	80	Maplin Electronics	W12 0HS
07/10/15	09:21:34	07771966917	234:96:17:109	35227	23.218.220.133	80	Marks and Spencer	W12 0HS
07/10/15	09:22:19	07771966917	234:96:17:102	26559	94.245.104.73	80	NHS	W12 0HS



This information would never provide a full web browsing history of a suspect or victim. Nor would it ever provide the content of communications but as with traditional CD, would provide a starting point for further targeted lines of enquiry.

As with traditional CD, this data needs to be proactively retained since it is mostly unknown that a criminal act will take place. A large proportion of investigations carried out by LE are reactive, only starting once an alleged crime has been committed.

Draft Bill provisions for Law Enforcement

As stated in David Anderson's review 'a question of trust' the Law Enforcement requirement for Communications Data are to:

1. Link an individual to an account or an action
2. Establish a person's whereabouts
3. Establish how suspects or victims are communicating
4. Observe online criminality, and
5. Exploit data [to corroborate evidence, identify further investigative leads]

Clause 47 in the draft Investigatory Powers Bill enables the retention and restricted access (by Law Enforcement) to Internet Connection Records (ICRs) for the purposes of;

- identifying the sender of a communication (LE requirement 1&2),
- identifying the communication service a person is using (LE requirement 3), and
- determining whether a person has been accessing or making available illegal material online (LE requirement 4).

These provisions meet four of the five Law Enforcement requirements and are very welcome but there will remain crucial gaps in LE capabilities which restricts our ability to discharge our responsibility to protect the public.

The fifth LE requirement is crucial to investigations; often a suspect or victim is known and the investigative query is based on understanding their actions to enable further follow up lines of enquiry.

Access to ICRs to understand their digital footprint would provide investigative leads in the digital and real world. Restricting LEA from requesting this type of data significantly hinders the capability for LE to protect the public.

The limitations mean that although the data is retained, LEA will be unable to request all data concerned with an investigation. There could be further evidence that can identify or exonerate a suspect and/or locate a missing person that exists but which cannot be requested by Law Enforcement under the IP Bill provisions.

Law Enforcement remain concerned that such a restriction is incompatible with their ability to protect the public, or seek to bring about a fair trial.

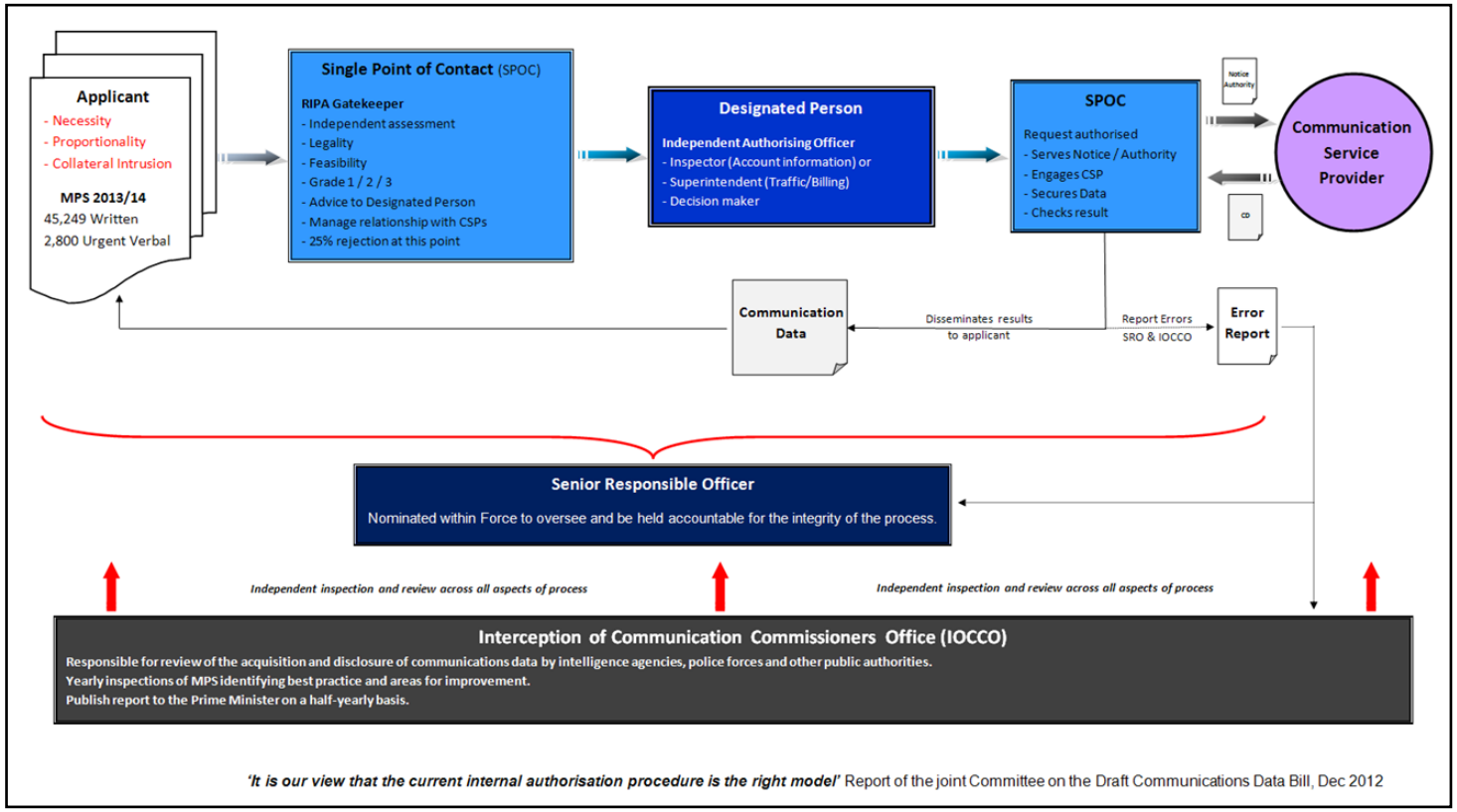
In seeking the authorisation of a request for communications data the applicant must demonstrate that the request is for a statutory purpose, typically for the prevention and detection of serious crime. As such, all applications are targeted towards those suspects or victims that are believed to be engaged in serious criminality or are at risk. Intelligence and evidence gathered through the

analysis of Communications Data therefore enables investigators to identify the actions of the suspect or victim within appropriate timescales and will be crucial to progress investigations.

When individuals use 'traditional' calls and texts no differentiation is made between the types of services accessed and data returned to Law Enforcement. There are hundreds of cases across all areas of serious crime where this information is important to investigations however the provisions of the draft IP Bill place restrictions on the access and use of this data when it is online.

Annex D sets out the sort of challenges faced in day to day policing and investigation of serious crime related to for example missing persons, children and vulnerable people when the internet is used as a means of communication and access point to services that would otherwise have been made in the 'real world'. An assessment of how the draft IP Bill would impact these types of investigations has also been included as currently understood. A summary is included that shows the impact on proactive and reactive enquiries where law enforcement seek to exploit Communications Data not linked to either a Communications Service or accessing illegal material. This might include where details of planned travel, banking, and some online purchases (relevant to a crime but the possession of which would not of itself amount to a crime) all of which would establish a pattern of behaviour leading to a number of other enquiries. This is normal procedure for most investigations whether for a missing person or investigation into a crime where there might be a number of suspects.

Annex C – Authorisation Process for Accessing CD



Applicant A person linked to or the Investigator of a criminal offence, normally a Constable or member of Police Staff, who require Communications Data in order to complete investigations. They consider and record the elements of **necessity**, **proportionality** and **collateral intrusion**. Although necessity is an objective test, applicants are required to articulate how the application links to the crime or the individual concerned.

Single Point of Contact (SPoC) Accredited Individuals trained as guardians and gatekeepers for the process. The SPoC is independent of the investigation and dedicated to the process, they provide advice to the operation and also act as a focal point for Communication Providers. SPOCs grade the response according to threat - G1 (Immediate Threat to life), G2 (exceptionally urgent operational requirement, serious crime) and G3 (routine).

Designated Person Senior officer at a rank stipulated by Parliament, trained to consider the impact on human rights of acquisition. This individual must be independent from the investigation and considers both the application and advice from the SPoC to a standard that will withstand scrutiny.

Senior Responsible Officer (SRO) The process is overseen by the nominated SRO who is held accountable for the integrity of the process,

Interception of Communication Commissioners (IOCCO) Independent oversight body – independent of Government and Parliament - reviews the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities by conducting yearly inspections. Produces report to Prime Minister on a half-yearly basis.

Annex D - Threat Picture Operational Examples: Impact of the Communications Data clauses of the Investigatory Powers Bill

Crime: Child Sexual Exploitation and Abuse (CSEA)

CSEA remains a particularly significant threat, with every UK policing region reporting cases of contact child sexual abuse (CCSA) in 2014; the proliferation of indecent images of children (IIOC) and online child exploitation (OCSE) continue to subject children to risk.

Impact of the Internet: The current volume of referrals to the NCA of UK-based individuals sharing indecent images of children (IIOC) online, approximately 1,500 per month, is 25% higher than it was last year (and 275% higher than in 2010) and the volume of reports of contact abuse to police also continues to rise. These reports are often unable to be investigated due to the lack of data held by CSPs which would enable identification of individuals who have posted and shared IIOC. The live-streaming of abuse from developing to the developed world is judged to be an emerging threat as access to well-developed internet infrastructure (4G and broadband) increases.

Example: On September 11th 2015, seven men were convicted of child sexual abuse offences and handed sentences totalling 107 years as part of Operation VOICER. His Honour Judge Lambert said during sentencing that this case was 'evil beyond rational understanding'.

This investigation related to an organised crime group (OCG) which coordinated grooming and contact sexual abuse of extremely young infants, in addition to making and distributing Indecent Images of Children (IIoC). 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 identifying 262 other paedophiles involved internationally, a number of which remain unidentified. Usage of these applications is not shown in traditional communication data records.

Bill Provisions: The provisions in the draft Bill that enable ICRs to be requested would certainly assisted in an operation such as VOICER explained above. In this case, access to retained ICRs would have provided vital intelligence to identify who these people are and in turn identify their communications and further linked suspects to enable enforcement action and safeguarding of victims. It is also anticipated that this might have speeded up the investigation so preventing additional harm inflicted on the victims.

This investigation was reliant on seizing suspect devices revealing the extent of communications between child abusers. Much of this information would have been available proactively through CD if ICRs were retained.

Threat: Firearms

Despite reductions in the criminal use of firearms and discharges, the risk from firearms remains serious. Overall, there were 30 fatalities in 2012/13 resulting from offences involving firearms. Firearms continue to enter the criminal market through a variety of means, including direct importation through post/fast parcels and thefts from legitimate firearms holders or dealers.

Over a three month period (May to July 2015) the NCA Border Policing Command (BPC) received 220 detections of firearm seizures from Border Force. 54 of these seizures were firearms.

Impact of the Internet: Criminals acquire firearms from a range of sources, including online sellers (e.g. via the anonymous criminal marketplaces on the darkweb), at militaria fairs and through criminal contacts. Social media and TOR forums are often used as platforms for related discussions and this is of growing concern.

Project EAGLEHEAD is a joint investigation between the NCA and USA's Homeland Security Investigations (HIS) targeting US based sellers that supply UK customers. EAGLEHEAD has led to:

- The recovery of more than 58 firearms by 26 police forces
- The arrest of 21 people and charge of 19 people with firearms offences

Whilst projects such as EAGLEHEAD have been successful at having a positive impact on some US based sellers who are now refusing to sell to UK buyers the investigation is dependent on international cooperation where there is no legal basis for sellers to comply with UK requests and patchy retention of IP data that enables identification of both buyers and sellers.

At present when illegal firearms are found to be posted on legal sites the NCA issues an alert to the website requesting removal of the posting. Little else can be done to trace the individual who has posted these adverts if false account details are provided.

Example: An ongoing investigation into a firearms supplier on the dark web which identified a number of UK based customers is an example of how both the dark web (TOR) and open source websites are used as a source of illegal firearms such as assault rifles, submachine guns, ammunition and associated component parts.

Bill Impact: The draft Bill will enable ICRs to be requested for 'illegal sites' (definition to be clarified) however the restriction placed on wider investigative leads means that Law Enforcement will not be able to request ICRs for legal sites that may sell firearms from other jurisdictions or online marketplaces where Law Enforcement is reliant on 'tip-offs' from the general public or the website itself once an illegal sale is posted. This will leave a big gap in the intelligence picture for law enforcement and negatively impact the ability to trace the source of firearms supply and the networks that are purchasing them.

Threat: Human Trafficking

Human trafficking for sexual exploitation is estimated to cost the UK £890 million each year in addition to the misery inflicted on its victims.

Human trafficking and wider aspects of modern slavery remain a high-priority threat to the UK. Referrals of Potential Victims of Trafficking (PVoT) to the National Referral Mechanism have increased year on year for the past 3 years. The HO estimates that there may have been as many as 10,000 to 13,000 PVoTs in the UK in 2013. Labour exploitation was the most common trafficking type in the UK in 2014, it is likely to remain an increasing risk in 2015.

Impact of the Internet: The internet and mobile technology is now an integral part of the advertisement and 24 hour supply of men and women for all aspects of sexual services. Internet platforms are used for sex workers to advertise their availability and are also used by those who deliberately traffic men and women in and out of the UK for sexual exploitation.

In some instances the individuals who operate these websites take great steps to conceal their identity through obfuscation of the domain's registration details (unique address), similar to the use of off shore shell companies with nominal directors appointed. This is just as likely to be as a means to avoid the tax authorities and pressure from law enforcement than for any other purposes. Other sites are able and do provide intelligence to assist with Law Enforcement investigations.

Whilst overt use of the internet and mobile technology plays an integral role in many aspects of the sex industry (and the exploitation of victims), it is unassessed if the dark web is used in any coordinated way by human traffickers.

Example: An investigation into an Organised Crime Group suspected of involvement in controlling prostitution, human trafficking and money laundering in Northern Ireland with links to Europe highlights the use of the internet to facilitate a traditional crime.

The OCG used an online escort site to advertise the services of victims of trafficking hidden amongst a surplus of other consenting sex workers in order to generate criminal funds. The use of the internet in this case provided multiple evidence and intelligence gathering opportunities in relation to communications data.

Communications Data obtained in relation to these adverts included both traditional call data (telephone numbers) and IP data enabling the identification and location of the victims and organised crime group members. CD was used in conjunction with analysis of account information and photographs which were examined for metadata, common backgrounds, clothing and locations allowed PSNI to identify adverts on other websites around Europe.

Bill Provisions: In this example the investigation would have benefited from access to ICRs for the purposes of identifying additional communication sites that the suspects had visited as this would have provided leads on other sites

the sexual exploitation of victims of trafficking were being advertised and identification of the wider criminal network.

The restrictions in the IP Bill to request ICRs for wider investigative services would hamper the investigation since data on banking services used to launder proceeds of crime and travel bookings would have provided key leads of enquiry.

Threat: Missing Persons

The police deal with a missing person's incident every two minutes. Last year 10% of missing incidents (of 211,521 records in 43 forces) were classified as high risk: 60 high risk missing incidents each day of which around 40 will be children. High risk cases require the immediate deployment of police resources. The police investment in high risk cases is a serious resource and financial commitment. 70% of search advisor time is spent on missing incidents. A conservative estimate of the average cost of investigations in high risk cases is between £6,500 and £8,500 (more than £150m each year for all high risk cases).
Operational Response: Each of the high risk case investigations will include an assessment of both communications and financial data in the search for and safeguarding of the missing person.

Example: In a missing/abduction case involving a teenager in the north of England, a girl had arranged to meet an older man. The man had been in communication with the girl using numerous online methods with initial contact being made via PlayStation online forums with further conversations enabled via VoIP (Voice-over IP) within an online gaming capacity. It was information from the girl's data which identified the man's device and then identified the location and the hotel.

Bill Provisions: This case could have progressed more quickly with access to Internet Connection Records, especially as the police did not have access to the girl's phone. The communications between the man and his intended victims had been through chat rooms and internet messaging services and not voice or text calls. The case relied on evidence from Communications Data obtained from the seized `phones and computers, which could have been obtained proactively through ICRs.

In the case above, the Bill provisions would enable investigators to identify the online chat services that the missing child had accessed prior to her disappearance enabling follow up enquiries to be made to the providers of these services and ideally leading to identification of her abductor. However, the restriction on requesting ICRs for wider investigative leads means that Law Enforcement would not be able to request the supporting information on the services accessed by the victim or suspects device that could identify that they had looked at the hotel website and therefore provide investigative leads on where the victim could be located.

Threat: Tax Crime

The cost to the UK from organised criminal attacks on the UK's tax systems is currently estimated at over £5 billion per annum.

Impact of the Internet: Threats and risks to online tax systems are fuelled by anonymity and agility both of which the internet provides. Alongside 'traditional' smuggling and VAT fraud offences HMRC is seeing a growth in the number – and sophistication - of online attacks. Broadly these fall into two categories:

- The use of stolen identities to submit fictitious returns to generate repayments
- The use of login credentials stolen from customers to acces their accounts and divert repayments or steal confidential data.

In the first case, for example, stolen company payroll data can provide information required to register an unknowing victim for new tax accounts. At the point of registration with HMRC the victim's bank account details will be used but this is likely to be changed following confirmation of a successful login. The only realistic way of investigating this offence is by following communications data identifiers such as the IP address which will be produced at the point of online interaction between the criminal and HMRC. If CSPs do not keep IP address details then the trail will run cold.

In the second case identifying the criminal is the challenge. Access to the hijacked account causes the criminal's IP address to be logged. But more sophisticated criminals will take steps to thwart investigation by traversing through numerous IP addresses across different networks and physical locations.

Example:

HMRC conducted an investigation into an OCG utilising the Department's on-line platforms to register multiple Value Added Tax (VAT) and Income Tax Self Assessment (ITSA) applications using hi-jacked or bogus identities. The OCG masked their identities and locations by utilising internet cafes, WIFI hotspot areas and broadband from the addresses of friends and relatives, to access HMRC's on-line facilities. Once a registration was successful the OCG made small repayment claims which were then gradually increased if the initial repayment was achieved.

Bill Provisions: This operation highlights some of the difficulties HMRC have been experiencing with IP address resolution as in this case HMRC were unable to obtain the IP login histories of several key targets as a consequence the HMRC was unable to identify links in the criminal conspiracy and was not able to use CD to evidence association between conspirators during the subsequent court case.

The provisions in the IP Bill which enable ICRs to be used for IP address resolution would improve HMRC's ability to identify and track individuals who are defrauding the revenue of the UK.