Title: Investigatory Powers Bill: Communications Data	Impact Assessment (IA)
IA No: HO0203	**Date: 4 November 2015**
Lead department or agency: Home Office	**Stage:** Consultation
	Source of intervention: Domestic
Other departments or agencies: FCO, NIO, Cabinet Office, NCA, MPS, GCHQ, MI5, SIS, MOD, wider law enforcement	**Type of measure:** Primary legislation
	Contact for enquiries: investigatorypowers@homeoffice.gsi.gov.uk

Summary: Intervention and Options

RPC Opinion: Not Applicable

Cost of Preferred (or more likely) Option				
Total Net Present Value	**Business Net Present Value**	**Net cost to business per year** (EANCB on 2009 prices)	**In scope of One-In, One-Out?**	**Measure qualifies as**
-£187.1m	£0m	£0m	No	NA

What is the problem under consideration? Why is government intervention necessary?

The ability of law enforcement, armed forces and security and intelligence agencies to obtain access to communications data is vital to public safety and national security. Communications data plays a significant role in major crime investigation and in every major MI5 counter terrorist operation over the last decade. It can be used as evidence in court and is essential in bringing criminals to justice. The ability of public authorities to access communications data is eroding as the way people communicate, increasingly through the internet, changes. Government intervention is necessary to ensure continued availability of, and access to, this data in order to keep the public safe and to ensure clear safeguards are in place to govern its use.

What are the policy objectives and the intended effects?

The objective is that law enforcement, armed forces and intelligence agencies are able lawfully to access communications data, when necessary and proportionate to do so, to keep the public safe in the fight against terrorism and criminality as well as to protect vulnerable people. The Bill's provisions will increase the effectiveness of identifying people online including in cases where a vulnerable person is at immediate risk of harm; provide information on how criminals communicate with each other via the internet; assist identifying people who have accessed illegal content, such as child abuse imagery and ensure clear safeguards are in place around the access to and retention of communications data.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

Option 1: No new legislation. Public authorities can access CD on a targeted basis and the SIA in bulk under existing legislation.The provisions for internet protocol address resolution in the Counter-Terrorism and Security Act 2015 would still remain. In the continued absence of legislation, it will remain impossible to resolve IP addresses consistently and capability gaps in respect of this will remain. This means that the effectiveness of law enforcement agencies to protect the public will continue to be undermined.

Option 2: Maintain current powers and legislate to close capability gaps including the introduction of two new criminal offences. Option 2 will provide significant additional benefits to police, armed forces and law enforcement. We have worked closely with a range of bodies across the operational community who have consistently maintained that the absence of updated legislation is having a negative impact on their ability to protect the public.

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:** December 2021

Does implementation go beyond minimum EU requirements?			N/A		
Are any of these organisations in scope? If Micros not exempted set out reason in Evidence Base.	**Micro** No	**< 20** Yes	**Small** Yes	**Medium** Yes	**Large** Yes
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)			**Traded:** N/A	**Non-traded:** N/A	

I have read the Impact Assessment and I am satisfied that (a) it represents a fair and reasonable view of the expected costs, benefits and impact of the policy, and (b) that the benefits justify the costs.

Signed by the responsible Minister: ..... Date: 3/11/15

Summary: Analysis & Evidence

Policy Option 1

Description: Do nothing

FULL ECONOMIC ASSESSMENT

Price Base Year 2015	PV Base Year 2015	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: 0	**High:** 0	**Best Estimate: 0**

COSTS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	0		0	**0**
High	0		0	**0**
Best Estimate	0		0	**0**

Description and scale of key monetised costs by 'main affected groups'

This is the do nothing option. There are no additional monetised costs associated with this option.

Other key non-monetised costs by 'main affected groups'

This is the do nothing option. There are no additional non-monetised costs associated with this option

BENEFITS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	0		0	**0**
High	0		0	**0**
Best Estimate	0		0	**0**

Description and scale of key monetised benefits by 'main affected groups'

This is the do nothing option. There are no additional monetised benefits associated with this option

Other key non-monetised benefits by 'main affected groups'

This is the do nothing option. There are no additional non-monetised benefits associated with this option

Key assumptions/sensitivities/risks — **Discount rate (%)** 3.5

Changing communications technology and the expiry of existing legislation would likely result in the inability to acquire the data required in the fight against terrorism and criminality, with a consequential reduction in the rates of crime detection and criminal prosecution for cyber-enabled crime such as fraud, online child sexual abuse and hacking. Additionally it would result in declining public confidence of the safeguards surrounding the access to the data.

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			In scope of OIOO?	Measure qualifies as
Costs: N/A	**Benefits:** N/A	**Net:** N/A	No	NA

Summary: Analysis & Evidence

Policy Option 2

Description: Legislate to close capability gaps

FULL ECONOMIC ASSESSMENT

Price Base Year 2015	PV Base Year 2015	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: N/K	**High:** N/K	**Best Estimate:** –187.1

COSTS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low		10		**N/K**
High				**N/K**
Best Estimate	**169.1**		**6.6**	**187.1**

Description and scale of key monetised costs by 'main affected groups'

Description and scale of key monetised costs by 'main affected groups'

No costs associated with the current acquisition regime for communications data, both targeted and in bulk. New cost components include getting the relevant communications data from service provider systems for new provisions, building solutions to store the relevant communications data, running and maintaining the above.

Other key non-monetised costs by 'main affected groups'

There will be minimal business change costs associated with each of the new capabilities, such as training for operational personnel. There will be minimal costs incurred to the justice system associated with the creation of new offences.

BENEFITS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low				
High				
Best Estimate	N/K		N/K	**N/K**

Description and scale of key monetised benefits by 'main affected groups'

N/A

Other key non-monetised benefits by 'main affected groups'

There will be benefits derived from the additional areas of communications data capability to investigations leading to safeguarding children, disrupting cyber enabled crime, counter-terrorism, and the seizure of criminal assets. The additional safeguards being implemented ensure that clear safeguards are in place to protect the privacy of the public.

Key assumptions/sensitivities/risks — **Discount rate (%)** 3.5

Technical complexity can increase projected costs. There is also a risk that technical solutions will be outpaced by technical change and/or changes in consumer behaviour.

BUSINESS ASSESSMENT (Option 2)

Direct impact on business (Equivalent Annual) £m:			In scope of OIOO?	Measure qualifies as
Costs: N/A	**Benefits:** N/A	**Net:** N/A	No	NA

Evidence Base

A. Problem Under Consideration

Communications data (CD) is the context, not the content of a communication: who was communicating; when; from where; and with whom. It includes the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. CD is currently defined in the Regulation of Investigatory Powers Act 2000 and is legally distinct from a communication's content. It does not include the 'what' – i.e. the content of any communication – the text of an email or a conversation on a telephone.

CD is absolutely fundamental to ensure law enforcement and security and intelligence agencies are able to investigate crime, protect the public and ensure national security. It is used by law enforcement, the armed forces and security and intelligence agencies in the investigation of many types of crime, including terrorism – by law enforcement on a targeted basis, and by the security and intelligence agencies on both a targeted basis and in bulk. It enables them to understand the activities, contacts and whereabouts of a person who is under investigation. For instance, CD has played a significant role in the investigation of a very large number of the most serious and widely reported crimes, including the Oxford and Rochdale child grooming cases, the murder of Holly Wells and Jessica Chapman, the 2007 Glasgow Airport terror attack, and the murder of Rhys Jones. Where an investigation starts with an internet communication, such as in online child sexual exploitation cases or identifying the location of people at risk of imminent harm, CD will often be the only investigative lead. If this data is not available, these cases will go unsolved.

Access to CD by law enforcement and the security and intelligence agencies (and other relevant public authorities) is primarily regulated by the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA places strict rules on when, and by whom, data can be obtained and provides authorities with a framework for acquiring CD which is consistent and compatible with the UK human rights obligations. The processing of personal information, including CD, and the storage of personal data by industry is also subject to the Data Protection Act 1998 (DPA).

The evolution of the internet, mobile communications and personal computing has changed the way that people communicate and re-shaped the communications industry. This has created a less stable and faster changing communications environment with a much wider range of companies providing services.

These changes in the way people communicate means that the government needs to legislate to enable law enforcement and the security and intelligence agencies to continue to access and exploit the crucial relevant communications data that they need in order to continue to investigate and prosecute people committing some of the worst types of crime. This includes for example, terrorism, child sexual exploitation and murder. Communications data is equally vital to ensure public authorities' continued ability to locate missing and vulnerable people, to identify suspects or exonerate those at the scene of a crime.

In order to maintain the operational capabilities of law enforcement, it is essential that they can access communications data from communications service providers wherever those providers are based, on a targeted basis and for the security and intelligence agencies both targeted and in bulk.

B. Rationale for Intervention

DRIPA expires on 31 December 2016 and legislation is necessary to ensure that the government continues to be able to compel communication service providers to retain communications data where necessary and proportionate to do so.

The UK continues to face significant threats from serious and organised crime and terrorism. These threats span "old" crimes using new technology to new threats such as cyber-dependent and cyber-enabled crimes. These threats are accentuated by the rapid and persistent expansion in the development and adoption of new communications technologies, which continue to transform government, business and the ways in which we interact with each other. They afford a level of privacy that protects citizens but makes it easier for criminals to conceal their activities.

As technology continues to evolve and the way people communicate changes, so the capability of law enforcement and others to obtain access to communications data under the existing legislative framework continues to erode. Legislation is needed to address those challenges whilst continuing to have regard to the privacy of citizens.

Three independent reviews have been undertaken and published in the last year relating to the use and oversight of investigatory powers, including communications data: that by the Intelligence and Security Committee of Parliament, published in March of this year; that of David Anderson QC, the Independent reviewer of Terrorism Legislation, published in June; and that by the Royal United Services Institute, published in July. All three reviews have recommended that new legislation be brought forward to regulate the retention and acquisition of communications data.

David Anderson said, in respect of access to communications data:

'20. In relation to interception and the acquisition of communications data, the following types of compulsory warrant and authorisation should be available:

(b) For the acquisition of communications data in bulk, a bulk communications data warrant

(c) For the acquisition of communications data otherwise than in bulk, an authorisation' (Page 289, David Anderson 'A Question of Trust')

He said in respect of bulk communications data:

'To give an example of a circumstance in which [bulk communications data] might apply, bulk communications data is essential in identifying and illuminating particular types of activity on a network for the purposes of cyber-defence, where GCHQ is seeking to identify malicious activity on particular networks. This activity neither targets nor meaningfully intrudes into the communications of individuals. But more generally, such a warrant is self-evidently less intrusive than the current s8(4) warrant'. (Pg. 276, David Anderson, 'A Question of Trust')

C. Policy Objectives

The objective is that law enforcement agencies, armed forces and security and intelligence agencies are able lawfully to access crucial communications data they need in the fight against terrorism and criminality, as well as to protect vulnerable people, when necessary and proportionate to do so. The retention of additional categories of communications data required will increase the effectiveness of law enforcement to investigate crime taking place on or enabled by internet communications including identifying the sender of an internet communication, often in cases where a vulnerable person has been assessed as being at immediate risk of harm, provide information on how criminals are communicating with each other via the internet, and assist in identifying people who have accessed illegal content, such as child abuse imagery or material encouraging or glorifying terrorism. Legislation will consolidate the statutory basesfor the acquisition of targeted communications data by public authorities, and the statutory bases for the acquisition of communications data in bulk by the security and intelligence agencies.

It will also provide for increased safeguards, including:

- The ability to share Single Point of Contacts (SPoCs) – Require infrequent users of communications data to set up collaborative agreements with more frequent and experienced users to enable shared services and to take advantage of expert advice;
- Streamlining access to communications data so that it can only be obtained through the new legislation;
- Creating an avenue of appeal for communications service providers to the Technical Advisory Board (TAB) on data retention notices;
- Extending the role of the Investigatory Powers Tribunal to cover the retention of communications data as well as the acquisition of communications data;
- Requiring communications data requests for the identification of journalistic sources to be approved by a judicial commissioner;
- Introduction of a new criminal offence which will carry a maximum sentence of 2 years imprisonment for knowingly or recklessly obtaining communications data from a telecommunications operator or postal operator without lawful authority;
- Introduction of a disclosure provision that will ensure that a communication service provider does not notify the subject of an investigation that a request has been made for their data unless expressly permitted to do so.
- Allowing for automated systems to process and analyse communications data needed to answer more complex requests where data from different communications services might be required. It will ensure that, after analysis, only the data which identifies the key facts about a communication is passed to a public authority and data irrelevant to the investigation is destroyed.

New legislation will also have the objective of responding to specific communications data-related recommendations made by David Anderson, RUSI and the ISC.

D. Options

Two options have been considered for legislation.

Option 1: Do nothing.

This is the baseline option: It will mean that law enforcement would have access to existing capabilities and that nothing would be done to close the growing capability gap in respect of internet-based communications. The expiry of the existing data retention legislation would have a further significant impact on law enforcement ability to investigate crimes. Public authorities would continue to exercise powers of acquisition of targeted communications data, and the security and intelligence agencies to do so in respect of bulk communications data.

Option 2: Legislate to close capability gaps and provide for greater safeguards on communications data

This option would retain the ability of public authorities to acquire communications data, including for the security and intelligence agencies, to do so in bulk, as in option one. It would also retain provision for communications data retention.

This option would include a number of new provisions:

- **Internet Connection Records:** Legislate to allow the retention of internet connection records: data identifying internet communications services that have been used by an individual. This will provide significant additional benefits to police and law enforcement. We have worked closely with a range of bodies across the operational community who have consistently maintained that the absence of internet connection records is having a negative impact on their ability to protect the public. Local authorities will be prohibited from acquiring internet connection records.
- **Request Filter:** A safeguard which will be used to ensure that, after analysis, only the communications data which identifies the key facts about a communication is passed to a public authority and data irrelevant to the investigation is destroyed.
- **Introduction of a new offence of wilfully or recklessly obtaining communications data:** This will prohibit the misuse of capabilities by public authorities and will provide additional reassurance to the public.
- **Disclosure provision:** A provision that will ensure that a communication service provider does not notify the subject of an investigation that a request has been made for their data unless expressly permitted to do so. This would be backed by a criminal offence which will have a maximum sentence of 2 years imprisonment on conviction on indictment for a communication service provider to inform the person to whom a communications data request relates that such a request has been made without express permission.

Internet Connection Records

Internet connection records are communications data identifying communications services that have been used by an individual. They can help determine which uniquely identifiable device has been interacting with a specific internet service, i.e. a server holding illegal images, or which internet servers/services a device has been communicating with.

Such internet services may be provided by the network access provider e.g. AcmeUK email for an AcmeUK internet customer, or a third party such as AnyEmail.com or AnySocialMedia.com. If law enforcement can identify a subject of interest (for instance a suspect in an investigation), the internet connection records may be acquired from communications service providers where

necessary and proportionate to determine what internet services they were using at a given time.

By legislating for the lawful retention of internet connection records by communications service providers this will:

- Increase the effectiveness of internet address protocol resolution, including in cases where a vulnerable person has been assessed as being at immediate risk of harm;
- Provide information on how criminals are communicating with each other via the internet;
- Assist in identifying people who have accessed illegal content, such as child abuse imagery or material encouraging or glorifying terrorism.

Local authorities will be prohibited from acquiring internet connection records.

Request Filter

The Request Filter is a safeguard which will be used to process and analyse communications data needed to answer more complex requests where data from different communications services might be required.

The Request Filter is intended to enable law enforcement agencies to continue acquiring complex CD in a way that minimises collateral intrusion. It will automatically analyse communications data needed to answer more complex data requests where data from different communications services providers might be required. It will ensure that, after analysis, only the data which identifies the key facts about a communication is passed to a public authority and data irrelevant to the investigation is destroyed.

By using the Request Filter to automate the analysis, the amount of data passed to public authorities will be minimised, reducing the levels of intrusion and protecting privacy.

Disclosure provision

While in many cases it would be detrimental to the investigation if a communication service provider notified the subject of an investigation that a request for their data had been made there are cases where this would not be the case. The legislation provides for communication service providers to notify the customer in such circumstances where the public authority is content for them to do so. It also makes clear that it is an offence for a CSP to notify the subject where no such permission is given.

E. Appraisal (Costs and Benefits)

The communications landscape and the way people communicate is constantly changing. The volumes of data being generated are increasing, and applications enabling people to communicate over the internet are developing constantly. This legislation will bring significant operational benefits to law enforcement, reducing the number of investigative enquiries that communications data cannot resolve.

Government has conducted consultation with public authorities, CSPs and other industry groups to understand the requirement, costs, benefits and technological challenges of implementing the provisions on communications data within the Investigatory Powers Bill.

In particular, consultation continues on the potential requirements that could be placed on CSPs under the proposed legislation and the market assumptions underlying the costs of implementing the clauses within the draft Bill. The consultation undertaken to date has openly examined the cost assumptions which have been reached within this impact assessment. The feedback has been supportive, confirming the suitability of the assumptions

The Government has also consulted civil liberties groups to hear their views on the scope of the legislation and the safeguards they consider should apply

Consultation also continues with public authorities to ensure a clear case can be produced to evidence the operational requirement for the capabilities provided for.

GENERAL ASSUMPTIONS AND DATA

The communications industry, communications technology and communications usage are all changing quickly. This makes estimating costs and benefits uncertain. The calculation of costs is in line with HM Treasury Green Book guidance, and include discounting at 3.5%. The costs outlined below are also without allowing for inflation, value added tax and depreciation. Optimism bias (OB) is applied in mitigation against projects and programmes being over optimistic about project costs and duration.

It is difficult to monetise the expected benefits of the CD provisions in the Bill. However we have consulted with several public authorities, including police forces, the National Crime Agency and the security and intelligence agencies to understand the impact of the legislation on their investigative ability.

GROUPS AFFECTED

- Communications Service Providers (CSPs)
- Law Enforcement Agencies (LEAs)
- Security and Intelligence Agencies (SIAs)
- Other designated Public Authorities using communications data
- The Interception of Communications Commissioner and the Information Commissioner;
- The general public, whose safety and security are affected by the capabilities of the police and other agencies to prevent and detect crime, and whose privacy needs to be protected.

Option 1: Do nothing

COSTS

Option 1 is the baseline. There would be no additional monetary costs or benefits under this option, as the acquisition of communications data both targeted and in bulk would remain on its existing statutory footing. The risks of doing nothing would include:

- The inability of law enforcement, armed forces and securityand intelligence agencies to acquire the additional data they need in the fight against terrorism and criminality and to protect the public.

- An ongoing reduction in the rates of crime detection and criminal prosecution for cyber-enabled crime such as fraud, online child sexual abuse and hacking
- A significant and worsening impact on the ability of law enforcement, armed forces and security and intelligence agencies to establish whether subjects of interest have accessed particular illegal content, and the "where and who" in the real world was using an IP address at a given point in time.
- Reduced public confidence in the transparency and safeguards surrounding the communications data acquisition and retention regime.

BENEFITS

This is the baseline option. There would be no additional monetary or non-monetary benefits to this option.

Option 2: Legislate to close capability gaps and improve safeguards

This option will allow the retention of additional data by domestic CSPs who are under a data retention notice. The retention of this additional data will ensure that law enforcement and intelligence agencies continue to have the powers they need to acquire communications data as threats change and technology develops. This option will also provide for additional safeguards in the acquisition of communications data, and a new criminal offence.

COSTS

Our best estimate of the total discounted cost of these policies above the baseline over the 10 year period is **£187.1m** (present value). A discount rate of 3.5% has been applied to this cost, in accordance with HMT Green Book guidance.

Included in these costs is the build and maintenance of the IT capability required to acquire and disclose the relevant data relating to ICRs, the build and maintenance of the request filter system providing additional safeguards, and storage costs of the data being retained. The table below presents a more detailed picture of the cost of each policy:

Table 1 – Summary of Estimated Costs

Economic Costs (£m)	**Transition Cost**	**Average Annual Costs** (excl Transition)	**Total Over 10 Years**
Internet Connection Records (Constant)	164.4	5.6	220.3
Request Filter (Constant)	4.7	1.0	15.0
Total (Constant)	**169.1**	**6.6**	**235.3**
Internet Connection Records (Discounted)	130.6	4.4	174.2
Request Filter (Discounted)	4.4	0.9	12.9
Total (Discounted)	**135.0**	**5.2**	**187.1**

We are continually engaging with key stakeholders to further refine these cost estimates.

There will also be business change costs associated with each of these capabilities. Staff will need to be provided with the relevant knowledge, skills and training to use internet-derived communications data successfully. These costs can vary but we anticipate will be small; they are not included in the above estimates.

Estimated Cost of New Offences:

Two new offences are proposed under this Bill:

1. A new criminal offence which will carry a maximum sentence of 2 years imprisonment for knowingly or recklessly obtaining communications data from a telecommunications operator or postal operator without lawful authority;
2. A provision that will ensure that a communication service provider does not notify the subject of an investigation that a request has been made for their data unless expressly permitted to do so backed by a new criminal offence which will have a maximum sentence of 2 years imprisonment on conviction on indictment.

Initial analysis from the Ministry of Justice suggests that the cost per defendant for each additional prosecution for either of the new offences could be in the region of approximately £10,200 (2014/15 prices, rounded to the nearest £100). This includes impacts to the Crown Prosecution Service (CPS) (£2,400), Her Majesty's Courts and Tribunal Service (HMCTS) (£1,900), the Legal Aid Agency (LAA) (£900) and the National Offender Management Service (NOMS) (prison and probation costs also allowing for a pre-sentence report: £5,000).

Key assumptions/risks of the above offences costs:

- To model the flow of the new offences through the criminal justice system, the proxy offence of unlawful interception of a postal public or private telecommunication scheme (S.1(1), (2) & (7), Regulation of Investigatory Powers Act 2000) was used. This offence is also triable either way with a maximum sentence of 2 years imprisonment on conviction on indictment. This assumption is owned by the Home Office.
- The figures above provide an initial estimated cost per additional defendant proceeded against for each of the above offences. All costs are weighted to account for the proportion of defendants tried in either the magistrates' court or Crown Court. The cost provided is an estimated average cost of a proceeding from the beginning of that proceeding to the end of the case (whether the offender is found guilty or not and accounting for the range of disposals possible).
- As there were very low volumes of prosecutions for the proxy offence, data was analysed over a 10 year period (2005 to 2014). This means that prison costs are very sensitive to changes in the custody rate and the average custodial sentence length given
- It was also assumed that 100% of defendants are tried in the Crown Court.
- An assumption has been made that these cases are unlikely to be heard in a closed court, as this will not be a standard requirement across all parts of the proceedings. It is however possible that certain cases will have to be heard in a closed court, which means the standard prosecution and other associated court costs outlined above may not apply and could therefore underestimate costs for cases heard in this manner.

- Costs for each new offence have only been estimated for each additional defendant proceeded against as there is still uncertainty around volumes. Once there are more robust estimates of these then we can finalise the overall impact to the CJS.

Given the modelling of existing offences, we expect total costs to be minimal. These costs have not been included in the overall CD IA costs as a result.

BENEFITS

The benefits of the additional powers have been considered against five operational requirements of law enforcement. Each of these operational requirements is crucial in preventing and detecting crime and protecting the public.

The five law enforcement requirements in relation to communications data are:

- Linking an individual to an account or action;
- Establishing a person's whereabouts;
- Establishing how suspects or victims are communicating;
- Observing online criminality; and
- Exploiting data.

As set out above, the communications environment is changing to the use of Voice Over Internet Protocol (VoIP) and internet based messaging services rather than traditional means of telephony communication and communications data is also becoming increasingly fragmented. As a result, the ability of law enforcement and intelligence agencies to use communications data to investigate and prosecute crime, and protect the public, is becoming more difficult and they are seeing their capability reduce. The Bill will redress the shortfalls in capability through the retention of additional vital categories of internet communications data.

It is difficult to monetise the expected benefits of the CD provisions in the Bill. However we have consulted with several public authorities, including police forces, the National Crime Agency and the security and intelligence agencies to understand the impact of the legislation on their investigative ability.

Internet Connection Records

The main benefit derived from internet connection records would be the ability to establish how suspects or victims are communicating and observing online criminality. Internet connection records would record the websites and applications services used by an individual including times of use and potentially duration and data volumes. The internet connection records associated with a number of subjects of interest, or associated with one or more websites could be examined to understand illegal activity. The destination IP address and port recorded in internet connection records could be combined with other data to uniquely identify a user where otherwise IP address resolution would only be able to identify a shared device or IP. This would **not** mean retaining every individual's web-browsing history.

Case Study Exercise:
The National Crime Agency (NCA) and Metropolitan Police Service (MPS) conducted a two month exercise throughout July and August. This exercise used a sample set of live

investigations and over the two months, investigators have completed a template in relation to each case, recording details of the impact of not retaining internet connection records.

The work conducted with law enforcement over the two month exercise has shown that without the retention of internet connection records:

- Investigators are missing significant investigative opportunities;
- Are frequently only able to use communications data to establish fragmented, incomplete picture of how suspects are communicating online;
- Crucially it is not possible to establish the use of wider internet services of investigative value that are known to be used by suspected criminals and subjects of interest.

In the time available it has not been possible to assess all of the returned data for inclusion within this impact assessment. However, three case studies have been identified within this impact assessment and are included below:

NCA – Human Trafficking (Operation Bootfish)

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 use 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 communications data requests. In addition, it is believed that one of the suspects books travel for the group online but there are no details of how. The retention of internet connection records could assist in identifying what online services are being used to book these journeys. Investigators have no intelligence to show how the groups are using the internet and, as a result, they cannot confirm whether the group have further associates that might be of interest to the investigation.

Internet connection records would provide operational benefit to the investigation by demonstrating how the suspects are communicating online, which may lead to the identification of additional suspects.

MPS – Fraud:

This is an operation into a serious malware based fraud with potential financial losses standing at US$137,000,000. A predominant member of the organised crime group responsible has been identified as residing in the UK. It is known that this suspect uses an internet enabled device and it is believed 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 establish what online communications services this suspect uses through communications data requests. In the absence of this data being available, an undercover officer had to be deployed to identify communications services that had been used. Investigators have also stated that it would be useful to establish the online banking services being used by the suspect over the internet but, in the absence of the retention of internet connection records, this is not possible.

Internet connection records would provide operational benefit to the investigation by preventing the need for directed surveillance on the suspect and by identifying what banking services had been used online.

MPS – Fraud (Operation Kadenza):
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 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 banking app at a given point in time.

ICRs would have provided operational benefit to the investigation by acting as a further identifier, beyond provisions in the Counter Terrorism and Security Act, enhancing the chances of identifying the relevant individual.

Forensic examination of mobile phones:
The Metropolitan Police Service also conducted an examination of data from 27 seized mobile phones. This showed that the majority of those devices had communications applications installed, which could not be detected currently by communications data requests. This was due to the current legislative restrictions in place within the CTSA 2015 which excludes the retention of certain types of communications data.

Request Filter

Communications activity has become increasingly fragmented as people own more devices which connect across multiple communications networks using a wider range of communications applications. The communications data now needed to understand the "who, how, when and where" of a single communication may therefore no longer be held by a single communications provider.

The Request Filter is intended to enable law enforcement agencies to continue acquiring complex CD in a way that minimises collateral intrusion. It will automatically analyse communications data needed to answer more complex data requests where data from different communications services providers might be required. The Request Filter will ensure that, after processing, only the key communications data is passed to a public authority and data irrelevant to the investigation is destroyed. By using the Request Filter to automate the analysis, the amount of data passed to public authorities will be minimised, reducing the levels of intrusion and protecting privacy. Without these filtering arrangements, public authorities are likely to need to make more requests to CSPs in future. They would need to piece the communications data together in-house requiring significant amount of resource time, with implications for personal privacy and data protection.

An example of the benefit the Request Filter could provide is shown by the following example:

> During a live terrorist investigation, if a law enforcement agency wanted to identify a suspect who they know was at two separate locations at two specific times, they might currently need to submit separate requests to a number of CSPs to obtain a full list of all those devices at each location, then compare these lists to see which device was in both locations. Under the proposed arrangements the filter would receive the required data from the CSPs and automatically analyse these returns without human intervention. Once the analysis had taken place, only the details of devices which were active in both areas at those times would be sent back to the investigating officer. The filter would then delete all the data, only retaining an audit trail of the relevant request data.

Communications data is used in a wide variety of investigations to protect the public and national security. An overview of the contribution CD makes to day-to-day operational activity, and how the measures in the Bill will improve the ability of police forces and the agencies to achieve these outcomes is summarised below:

Child Sexual Abuse (CSA) Disrupted

Where an investigation starts with an internet communication, such as in online child exploitation cases, communications data is often the only investigative lead available to law enforcement. The Child Exploitation Online Protection Centre (CEOP) estimates that there were some 50,000 individuals in the UK engaged during 2012 in downloading and sharing indecent images of children, often using decentralised or peer-to-peer (or P2P) networks. The Bill would facilitate the identification of those involved and would be a significant contributor to the conviction of child offenders, for example:

> ***Case 4 from Annex 10 of the Anderson Report:***
> *Internet data were used in an investigation into the grooming of a 13-year-old girl on an internet chat service. Examination of the victim's computer by the authorities revealed the email address of a man who had coerced the girl into sending naked photographs of herself and exposing herself during webcam chat. Police officers made enquiries about the e-mail address which revealed the IP address belonged to an address in Wales. Further investigation resulted in the man being charged, preventing potentially more serious sexual offences taking place.*
>
> The surge in the use of communications services from overseas providers has meant that police forces increasingly require access to extra-territorial data for cases similar to the one above. This Bill will provide this capability, ensuring that CSA cases can continue to be investigated as effectively as possible. The retention of ICRs could also have increased the investigative picture, quickly revealing whether the man had been accessing other illegal websites with content such as

child abuse imagery.

Counter Terrorism (CT)

The provisions in the Bill could reduce the risk of terrorism, by providing law enforcement and the security and intelligence agencies with the ability to identify terror suspects, who may be communicating with each other for attack planning purposes using internet communications that under existing legislation would make them anonymous. The provisions in the Bill would also enable the identification of people who have access particular illegal content relating to terrorism, such as material giving terrorism-related instructions.

It is cited in the Anderson report that the significance of messaging and social media in terrorism prosecutions is immense. The Crown Prosecution Service reviewed a snapshot of recent prosecutions for terrorist offences and concluded that in 26 recent cases, of which 17 have concluded with a conviction, 23 could not have been pursued without communications data and in 11 cases the conviction depended on that data. Giving law enforcement and the security and intelligence agencies the capability to investigate online crime more effectively could lead to the prevention of an attack on the UK.

A terrorist attack can have a large impact on the UK, both in terms of the immediate impact, such as lives lost, damaged infrastructure and lost output, and longer term costs such as higher public anxiety.

Resolving Threat to Life Cases

Communications data retained under the provisions in the Bill may form part of investigations where a person's life might be endangered if urgent action is not taken. These are known as 'threat to life' cases, and could include situations where a vulnerable person may intend to take their own life, missing person's cases or kidnapping. In David Anderson's report 'A Question of Trust', Police Scotland revealed communications data was used in over half of all threat to life incidents in Scotland in the latest three-month period.

The change in the way people communicate has meant that vulnerable people will often post their intentions to self-harm on social media websites, and subjects of interest may use VoIP or other internet based messaging services rather than traditional means of telephony to communicate. Communications data retained under the Bill will enable law enforcement and other emergency services to locate these vulnerable people quickly.

Cyber-Enabled Crime Prevented or Disrupted

Communications data is necessary in investigations into cyber-enabled crime, such as fraud, cyber bullying and hacking. The identification of suspects in these crimes can only be carried out using communications data, and the additional data retained under the Bill would enable this to be carried out more efficiently.

In a survey of 2000 web users last year by the Get Safe Online organisation, 51% admitted to having been in some way affected by online cyber scams, such as fraud, ID theft, hacking, online abuse or having their computer infected with a virus. The Bill may reduce the economic loss to individuals who are victims of these crimes.

G. Risks

Any programme to maintain access to communications data will be technically complex and there is a risk that technical solutions will be outpaced by technical change and/or changes in consumer behaviour. Capabilities to maintain access to communications data will need to be developed incrementally, with regular assessment of costs and benefits. They will be tested in small scale pilots in advance of larger procurement. Solutions will be flexible so they can be updated to reflect internet behaviour. Risks will be further mitigated by continued close partnership with the communications service providers, facilitated by legislation that will provide a sound legal basis for communications service providers' data retention and storage.

H. Implementation

The Government will introduce a Bill following any revisions necessary after pre-legislative scrutiny, in the New Year. The Bill will need to be enacted by 31 December 2016, by which point the Data Retention and Investigatory Powers Act will fall away.

I. Monitoring and Evaluation

The proposed legislation will be scrutinised by a Joint Committee of Parliament, before being introduced in the early New Year. The application of the legislation will be scrutinised on an ongoing basis by the Investigatory Powers Commission, an independent body of the judiciary, responsible for oversight of the use of investigatory powers by all public authorities, who will provide yearly reports on the exercise of powers within the Bill. The Intelligence and Security Committee of Parliament will continue to oversee the activities of the security and intelligence agencies, including their exercise of investigatory powers. And the Investigatory Powers Tribunal will provide a right of redress to any individual who believes they have been unlawfully surveilled.

J. Feedback

The Government will consider carefully the recommendations of the Joint Committee before bringing forward revised proposals for Introduction. Public consultation will form part of the pre-legislative scrutiny process.