Title:	Impact Assessment (IA)
Counter Terrorism and Security Bill - Internet Protocol Address Resolution	**Date:** 28/10/14
IA No: HO0136	**Stage:** Development/Options
Lead department or agency: Home Office	**Source of intervention:** Domestic
	Type of measure: Primary legislation
Other departments or agencies: Law Enforcement, Security and Intelligence Agencies.	**Contact for enquiries:** CTSBill@homeoffice.x.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, Two-Out?**	**Measure qualifies as**
-£98.9m	Minimal	Minimal	No	NA

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

On 29 August the Joint Terrorism Analysis Centre raised the UK threat level from SUBSTANTIAL to SEVERE meaning that a terrorist attack is 'highly likely'. There is a need to legislate to deal with the increased terrorist threat. The ability of the law enforcement, security and intelligence agencies to obtain access to communications data is vital to public safety and national security. Communications data has played a significant role in major crime and in every major Security Service counter terrorist operation over the last decade. It can be used as evidence in court and is essential in bringing criminals to justice. Our ability 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, primarily for the police.

What are the policy objectives and the intended effects?

The objective of these provisions is, with appropriate safeguards and protections, to address an important cause of the reduction in capability by relevant public authorities designated by Parliament to access communications data. The intended effect is that law enforcement and intelligence agencies have the powers they need to protect the public and ensure national security by being able to continue to identify a user or device from the service they have used, when necessary and proportionate to do so. The effects will not address all of the issues raised by technological change but it will provide a crucial component of tackling crime in the modern world.

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. There is limited scope under existing legislation to address the gap in available communications data.
Option 2: Legislate on internet protocol address resolution, to allow the retention of the relevant records so that, where necessary and proportionate, public authorities can identify individuals from their activities online.
Option 3: Legislate as with option 2, to allow IP address resolution, and also to close the other elements of the communications data capability gap: data identifying internet communciations services that have been used by an individual and data from overseas providers of services to users in the UK.
In the absence of agreement on Option 3, Option 2 will make a significant impact to a number of cases that otherwise could not be successfully investigated.

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:** 12/2016

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** Yes	**< 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/K	**Non-traded:** N/K	

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible Minister: ..... Date: .....

Summary: Analysis & Evidence

Policy Option 2

Description: Legislate on internet protocol address resolution, to allow the retention of the relevant records for the identification of subjects of interest to law enforcement whose identity would otherwise be hidden.

FULL ECONOMIC ASSESSMENT

Price Base Year 2014	PV Base Year 2014	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: -	**High:** -	**Best Estimate:** -98.9

COSTS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	-		-	**-**
High	-	4	-	**-**
Best Estimate	26.6		9.6	**£98.9**

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

The communication service providers most likely to be affected by this legislation have been consulted, including on the assumptions and high level costs estimates, and will continue to be included discussions on the implementation. The likely cost components include: getting IP data from service provider systems; building a solution to store the IP data at service providers; and running and maintaining the above.

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

-

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

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

-

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

There will be benefits derived from the use of IP address resolution to investigations leading to safeguarding children, disrupting cyber enabled crime, counter-terrorism, and revenue loss prevented. Further benefit will be gained due to the support that communications data will provide to investigations into financial crimes, saving lives and investigations leading to the seizure of criminal assets.

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

Assumptions and Risks are detailed in the evidence base. Key risks are:

- Technical Challenges;
- Increasing costs;
- Business Change.

BUSINESS ASSESSMENT (Option 1)

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

Evidence Base

A. Strategic Overview

A.1 Communications Data

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 number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. 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 defined in the Regulation of Investigatory Powers Act 2000 and is legally distinct from a communication's content.

CD is absolutely fundamental to ensure law enforcement agencies are able to investigate crime, protect the public and ensure national security. It is used by the police and intelligence agencies in the investigation of many types of crime, including terrorism. It also enables the police to build a picture of 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 retained, these cases will go unsolved.

The retention of CD in the UK has been recognised as a valuable and important measure for a number of years. 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).

Increasingly, the police and others are unable to get access to relevant CD. Changes in technology dictate the way people communicate in the modern world. This means that CD is becoming fragmented, with data about a single communication spread across various networks and services.

The change in the way people communicate means that law enforcement and intelligence agencies need to adapt their investigative techniques in order to continue identifying people committing some of the worst types of crime, such as terrorism, child sexual exploitation and murder. One of the key challenges for an investigator in solving internet based crime is the ability to identify who used a particular Internet Protocol address (IP Address), and where and when they used it.

Currently some of this important data is not retained by CSPs for their business purposes meaning that the data is not always available. New legislation is needed to require the CSPs to retain this important data.

A.2 Internet Protocol Address (IP address)

Most networks, including all computers on the internet use a protocol standard for how to communicate on the network. The unique identifier for a computer is called its IP address. An IP address is automatically allocated by a network provider to a customer's internet connection so that communications can be routed backwards and forwards to the customer. Combined with other technical identifiers this can identify a device/user.

By analogy, if a person were sending a letter by mail, an IP address could be considered to be the post code area where the letter needed to be delivered, and the other technical identifiers would indicate the specific door number and/or addressee.

A.3 The Background

On 29 August the Independent Joint Terrorism Analysis Centre raised the UK national terrorist threat level from SUBSTANTIAL to SEVERE meaning that a terrorist attack is 'highly likely'. Approximately 500 individuals of interest to the police and security services have travelled from the UK to Syria and Iraq since the start of the conflicts; a number of these individuals have joined terrorist organisations including the Islamic State of Iraq and the Levant (ISIL). On 1 September the Prime Minister announced that legislation would be brought forward in a number of areas to stop people travelling overseas to fight for terrorist organisations and subsequently returning the UK, and deal with those already in the UK who pose a risk to the public.

The UK Government first introduced legislation on CD retention in 2001. The Anti-Terrorism, Crime and Security Act 2001 (ATCSA) included at Part 11 provisions for a voluntary regime for the retention of CD by communications companies for longer than they would otherwise have done for their own business purposes.

The EU Data Retention Directive (Directive 2002/58/EC) passed into EU law in March 2006. This required European Member States to implement legislation into their own national law requiring communications companies to retain specific CD sets for retention periods between 6 and 24 months.

The EU directive was initially transposed into UK law for telephony only by the Data Retention (EC Directive) Regulations 2007. These were updated to include internet communications by the Data Retention (EC Directive) Regulations 2009 (DRR). These Regulations required UK communication providers to retain certain specified types of telephony and internet related CD which was generated or processed in connection with their business for 12 months.

In June 2012, the Government published for pre-legislative scrutiny a draft Communications Data Bill, which included provisions required to maintain the capability of law enforcement and other agencies to access CD. An Impact Assessment was published alongside the draft Bill.

The draft Bill was scrutinised by a Joint Committee of both Houses. The Intelligence and Security Committee (ISC) conducted a parallel inquiry into the draft Bill, which focused on its implications for the security and intelligence agencies. The Joint Committee published its report on 11 December 2012. A summary of the Intelligence and Security Committee's findings was published alongside the Joint Committee Report; and a redacted version of the full ISC report was published on 5 February 2013.

Both committees recognised the importance of CD to the police and the intelligence agencies; that not all the data required to support investigations was available and that legislation is

necessary to address the issue. Both committees, however, recommended changes to the draft Bill.

The Queen's Speech on 8 May 2013 stated "In relation to the problem of matching internet protocol addresses, my Government will bring forward proposals to enable the protection of the public and the investigation of crime in cyberspace."

On 8 April 2014, the European Court of Justice issued a judgment declaring the EU Data Retention Directive (DRD) invalid. Following the judgment, the Data Retention and Investigatory Powers Act 2014 (DRIPA) was passed on 17 July. The Act provides a clear statutory basis, in primary legislation, for the Government to require domestic communications service providers to retain certain types of CD. In addition the Act makes explicit that, as Parliament always intended, any company providing telecommunications services to customers in the UK must comply with lawful authorisations under Part 1 of RIPA, regardless of where those companies are based.

The Act also extends existing safeguards, enhancing the data retention notice regime and formalising the requirements on communications service providers to safeguard this crucial data. The legislation has replaced the Data Retention Regulations (EC Directive) 2009 with the Data Retention Regulations 2014, which came into force on 31 July. The Act does not enable the retention of any data types that could not be retained under the 2009 Regulations. In addition, the Regulations ensure that data can be retained for a maximum period of 12 months, enabling data to be retained by providers for a shorter period where appropriate in any given case.

DRIPA is a narrow and limited response to a set of specific challenges, providing a clear legal basis for existing powers. The Act, and the Regulations, do not create any new powers, rights of access, or obligations on communications service providers beyond those that already existed. The Act does not impact the capability gaps that we sought to address in the Draft Communications Data Bill. These capability gaps persist and are continuing to degrade the ability of our law enforcement and intelligence agencies' ability to do their jobs.

A.4 Groups Affected

The groups affected by these clauses in the Bill will be:

- 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; and
- 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.

A.5 Consultation

The pre-legislative scrutiny of the Draft CD Bill provided an opportunity for public consultation. The Joint Committee invited comment on specific questions and received a wide range of submissions; the majority were posted on its website.

Following pre-legislative scrutiny, the Joint Committee published its report on 11 December 2012 and made a number of recommendations to the draft CD Bill. Government conducted further consultation with industry, law enforcement agencies and interest groups to understand the implications of the Joint Committee's recommendations in terms of costs, benefits and technological challenges to implementing the full CD Bill.

Following the Queen's Speech on 8 May 2013, which identified that the government would bring forward proposals to enable the protection of the public and investigation of crime in cyber space, further consultation has taken place with domestic CSPs. This consultation has focused on the costs of solutions for implementing IP address resolution, and the technological challenges. Further meetings will be necessary to consult on any phased implementation, and how this impacts each CSP with regard to competitive issues, and their perceived need for a level playing field across the customer base.

B. Rationale for intervention

Protecting the UK against terrorism is a fundamental role of Government. Counter-terrorism measures require judgments on the need to balance protecting the public with safeguarding civil liberties and dealing with sensitive issues of national security. Such judgments should not be left to the private sector. The private sector does not have the access to intelligence to understand the scale/nature of the threat.

It is the Government that manages sensitive information and intelligence on individuals that pose a terrorist threat and is responsible for the safety and security of UK citizens. Given the necessity of counter-terrorism measures, and the role of the Government to protect the public, the Government is uniquely placed to fulfil this role.

B.1 The Challenge

One of the key challenges for law enforcement in maintaining their capability to investigate crime is: the resolution of an IP address to identify the unique attributes necessary to answer the question of 'who' in the real world was using an IP address at a given point in time; and the attribution of those communications to locations.

As examples of the challenges facing law enforcement, the National Crime Agency had to drop at least 20 cases over a six month period due to an inability to access communications data. In 18 of these cases, an IP address was the only investigative lead. The investigations that were dropped included potential life-at-risk child protection cases and investigations into the distribution of indecent imagery of children.

Similarly, the Metropolitan Police Service had to cease at least 12 investigations over a three month period due to communications data capability gaps. Half of these were cases that started with an IP address, where an inability to resolve it to an individual caused the case to stop. A number of these cases were compounded further by the use of internet services provided by companies based overseas. These cases included an investigation into a potential paedophile, harassment cases and attempts to identify and locate an individual who had threatened to commit suicide. These cases demonstrate the damage that is caused by the inability to consistently resolve an IP address to an individual in the real world.

When the Joint Committee reported its findings following pre-legislative scrutiny it highlighted the importance of IP address resolution. They were clear that there would be a significant benefit to law enforcement if there were legislation that would enable the matching of an IP address to an individual subscriber.

The extract from the Joint Committee report stated "*The originating IP address of a communication is routinely gathered in many types of internet transaction, but* ***if the CSP does not hold information on which of its subscribers held which IP address at a particular point in time it is very hard for law enforcement authorities to prove an association between an action on the internet and a particular individual****. Not all United Kingdom providers currently obtain all the data necessary to trace which subscriber is using which IP address.* ***During the course of our inquiry we heard of various circumstances in which the lack of this data has impeded investigations.*** *We accept that if CSPs could be required to generate and retain information that would allow IP addresses to be matched to subscribers this would be of significant value to law enforcement. We do not think that IP address resolution raises particular privacy concerns.*" (emphasis added)

New internet-based technologies are generating communications data in different ways. Not all this data is retained by CSPs as they may have no business reason to do so. Changes in the way people communicate mean that CD is also becoming increasingly fragmented, with data about a single communications event distributed across several providers.
Consumers are also making greater use of communications which are moving away from traditional mobile telephony and text messaging to telephone calls which are made over the internet. These are commonly referred to as Voice Over Internet Protocol (VOIP). There is also a move away from traditional text messaging to Instant Messaging Services. The technology is constantly evolving and at this point in time, it is essential that legislation is passed to require CSPs to retain the data that allows law enforcement and security and intelligence agencies to attribute an IP address to a person, device and location, with the appropriate safeguards.
At the same time, communication over the internet can often be anonymous, requiring further data analysis in order to identify who made a communication, when and where. This means that it is vital to be able to determine the Internet Protocol (IP) address that a subscriber or device has used to access the internet.

An IP address is automatically allocated by a network provider to a customer's internet connection so that communications can be routed backwards and forwards to the customer. Domestic communications service providers (CSPs) may share IP addresses between multiple users. The providers currently have no business purpose for keeping a log of who used each address. It is therefore important that those logs are retained to enable the identification of the user of the IP address at a given point in time.

B.2 The response

The provisions in the Counter Terrorism Bill on IP resolution will ensure the retention of CD that is required to identify where and who in the real world was using an IP address at a given point in time. To make this possible the Bill will provide the lawful basis for UK service providers to retain sufficient IP data to allow law enforcement to attribute communications to locations as well as to people or their devices.

Individual CSPs may be given a notice by the Secretary of State to: obtain, process and retain communications data they would not ordinarily hold for their own business purposes (i.e. data necessary to link the unique attributes of a public IP address to a user or device); retain this data safely and securely; and hold the data in a way that facilitates efficient disclosure of the data to public authorities.

B.3 Safeguards

There are strict statutory safeguards covering the use of CD within existing legislation. The UK currently has in place one of the most rigorous CD oversight and authorisation systems in the world.

- CD may only be acquired under RIPA by public authorities that have been approved by Parliament to do so.
- CD may only be acquired for a specific purpose set out in RIPA (e.g. for the purpose of preventing or detecting crime, in the interests of national security or for the purposes of preventing death or injury in the case of an emergency).
- Acquisition of CD must be authorised by a senior officer at a rank stipulated by Parliament.
- The authorising officer may only authorise a request for CD if the tests of necessity and proportionality are met in that particular case.
- In the case of local authorities, requests for CD must also be approved by a magistrate, under provisions within the Protection of Freedoms Act 2012.
- The Interception of Communications Commissioner provides independent oversight of the acquisition of CD by public authorities, including through inspections of public authorities. He provides a (published) annual report to the Prime Minister. Provisions in DRIPA will ensure that the Commissioner will report twice a year in the future, further enhancing the transparency of our regime.
- The processing of personal information, including CD, is regulated by the Data Protection Act 1998, which is overseen by the Information Commissioner.

In relation to the safeguards contained in RIPA, the Joint Committee on the Draft Communications Data Bill commented:*"It is our view that the current internal authorisation procedure is the right model."*

In addition, DRIPA has introduced a number of additional safeguards to our already robust regime. These safeguards are:

- Specifying that Ministers must consider the necessity and proportionality before issuing a data retention notice to a communications service provider.
- Specifying further requirements around what information Ministers must consider before issuing a data retention notice.
- Amending the set period for which data is retained, from 12 months to a maximum of 12 months (allowing for shorter periods if there is lesser need).
- Limiting access to retained CD to requests under RIPA and court orders.
- Ensuring that data security requirements must be specified in a notice to each CSP, rather than in commercial arrangements as at present.
- Clarifying the duties of the Information Commissioner, so that he oversees the security, integrity and destruction of retained data.

C. Policy Objectives

The objective of these provisions is, with appropriate safeguards and protections, to address an important cause of the reduction in capability by relevant public authorities designated by Parliament to access communications data.

The intended effect is that law enforcement and intelligence agencies have the powers they need to protect the public and ensure national security by being able to continue to identify a user or device from the service they have used, when necessary and proportionate to do so. By requiring CSPs to retain sufficient data necessary to attribute an IP address to a location, the user and/or their device, will mean that law enforcement and intelligence agencies will continue to have the capability to investigate crime in cyber space.

The effects will not address all of the issues raised by technological change – it will not address all elements of the growing CD capability gap – but it will provide a crucial component of tackling crime in the modern world.

D. Options

Option 1: no new legislation

Under this option the acquisition of CD by UK law enforcement and intelligence agencies would continue to be on the basis of existing legislation. There is limited scope under existing legislation to address the issue of IP address resolution.
This option would mean:

- There would be insufficient CD available for law enforcement to undertake investigations. Continued degradation of the lawful capability to acquire CD;
- A significant impact on the ability of law enforcement and intelligence agencies to identify the unique attributes necessary to answer the question of 'where and who' in the real world was using an IP address at a given point in time;
- A reduction in the rates of crime detection and criminal prosecution for cyber enabled crime.

Option 2: Require communication service providers to retain data necessary to attribute an IP address to a user of an internet access service and a wider range of internet services.

To protect the public, new legislation being introduced that maintains the ability of law enforcement and intelligence agencies to protect the public and support the investigation of crime in cyberspace. This will be achieved by:

- Introducing new requirements on CSPs to retain CD, including beyond their own business need;
- Amending the Data Retention and Investigatory Powers Act 2014 (DRIPA) to enable communications service providers (CSPs) who provide an internet service to retain data necessary to attribute an IP address to an individual;
- Expanding DRIPA to cover a wider range of internet services.
- Providing payments to be made to CSPs in respect of costs incurred in complying with new legislation

Option 3: Require communications service providers to retain the full range of CD that is required to allow for efficient and effective access by public authorities when necessary and proportionate to do so.

To protect the public, new legislation would ensure that the capabilities to acquire CD retained by CSPs are maintained by:

.

- Introducing new requirements on CSPs to generate, obtain, process and retain CD, including data beyond their own business need;
- Enabling CSPs who provide an internet service to retain data necessary to attribute an IP address to an individual, as well as the data necessary to close the wider CD capability gaps;
- Providing new arrangements to facilitate the secure, efficient and effective transmission of CD to public authorities;
- Providing payments to be made to CSPs in respect of costs incurred in complying with the new legislation.

Option 2 is the chosen option

Option 3. It has not been possible to gain agreement to introduce this option.

E. Appraisal (Costs and Benefits Best Estimates)

One element of the CD Bill was to maintain the capability of law enforcement to identify who was using an IP address and where they were using it at a given point in time; consultation took place during this time. The communications landscape and the way people communicate have constantly changed. The volumes of data being generated are increasing and applications enabling people to communicate over the internet are developing constantly.

Further consultation has taken place across industry since the publication of the Joint Committee's report. This has included, earlier this year, a study into the costs likely to be associated with implementation of IP address resolution with UK based CSPs.

However, it has proven challenging to monetise the benefits, particularly as part of an emergency Bill package. We continue to work with law enforcement to better understand the uplift in capability that IP address resolution on its own will provide.

There is no doubt that IP resolution legislation will be a significant contributor to maintaining an effective CD acquisition service. However, it is still expected that without further legislation that includes provision for the retention of weblogs data or destination IP address, there will remain a number of investigative enquiries that cannot be resolved using CD. The benefits achieved by IP resolution should be treated within the context of this larger potential capability that could be achieved should additional legislative change be implemented in the future.

E.1 General Assumptions and Data

The communications industry, communications technology and communications usage are all changing quickly. Estimated costs and benefits may change and will continue to be subject to regular review. The costs outlined below are without allowing for inflation, value added tax and depreciation. The calculation of those costs is in line with HM Treasury Green Book guidance. Optimism bias (OB) is applied in mitigation against projects and programmes being over optimistic about project costs and duration.

E.2 Costs Option 2:

The costs are based on studies conducted by industry. The *present value* of costs over a 10 year period is estimated to be £99 million; this figure may change with continued development in technology and services.

In *current prices*, the costs of implementing IP resolution at service providers will be in the region of £27m; the costs of running and maintaining these solutions is estimated to be £96M over the 10 years.

The totals above are based on:

1. Getting the IP data from service provider systems
2. Building a solution to store the IP data at service providers
3. Running and maintaining the above

The cost estimates for the individual components above are based on:

- Studies into IP resolution conducted by industry
- Prior work with service providers and industry on similar projects

Alternative methods of investigation, such as directed surveillance and undercover officers, cost significantly more than CD, do not provide the same level of benefit and are very often more intrusive.

E.3 Benefits Option 2:

As set out above, the communications environment is changing to use Voice Over Internet Protocol (VoIP) and internet based messaging services rather than traditional means of telephony communication and CD is also becoming increasingly fragmented. As a result, the ability of law enforcement and intelligence agencies to use CD to investigate and prosecute crime is becoming more difficult and they are seeing their capability reduce.

IP address resolution will redress some of the shortfall in capability through the ability to identify anonymous internet users. In particular:

a) Where Law enforcement agencies have accurate source information (eg IP address and accurate time) from an internet service provider they can identify which user sent that communication.
b) If law enforcement have multiple incomplete records (IP address and approximate time only) then they have a greater likelihood to identify which user sent the communications.
c) It would improve the number of cases where law enforcement agencies have accurate source information enabling them to resolve the IP addresses, as set out above. For example were a user uploads an illicit file to a cloud server that server provider, if subject to a data retention notice, would be required to retain sufficient information to enable the internet access provider to identify the user.

As a result, the use of IP address resolution in investigations would contribute towards:

Counter terrorism (CT)

A Police CT perspective:

Police CT
"Internet Protocol (IP) log-on data is used within most internet related CT investigations allowing us to identify the location of a wide variety of communication devices when Subjects of Interest (SOIs) are communicating via the internet. What is required now is the ability to identify what internet based services have been accessed by a SOI, how and where those services were accessed from and with whom they were communicating over those services."

IP address resolution 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.
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

Safeguarding children

Where an investigation starts with an internet communication, such as in online child exploitation cases, CD is often the only investigative lead available to law enforcement. IP address resolution capability presently available to law enforcement is a significant contributor to the conviction of child offenders. As the way people communicate is changing, the capability to be able to identify where and who was using a particular IP address at any given point in time is degrading. By requiring CSPs to retain sufficient data necessary to attribute an IP address to a location, the user and/or their device, will maintain the investigative capability of law enforcement.

This current capability has provided a significant contribution to law enforcement operations, for example:

- 'Police Scotland Internet Unit Child Protection has arrested and charged 300+ offenders for abusive images of children since April 2013 through IP resolution (equating to 200+ convictions per annum)' **where data has been available.**

Revenue loss prevented.
IP attribution will help to identify and subsequently prosecute perpetrators of fraudulent claims, which often use stolen identities, in relation to VAT, Income Tax Self Assessment and Tax Credits. It could contribute to stopping further fraudulent attempts.

> **HMRC**
> In 2013/14 HMRC's use of CD and LI prevented the systematic theft of over £1 billion from the public purse. Any debate about the necessity of resolving IP addresses must be seen in the context of HMRC's *digital-by-default* strategy, the department's ambition to move all of its services to customers fully online. Within government HMRC already has the biggest online presence and operates the largest number of critical national infrastructure systems. As more tax systems go online HMRC will become more and more vulnerable to cyber attack. And we will need the tools to do the job. Without IP address resolution our investigators will have practically nothing to go on in online cases. And you will see the impact on that £1 billion which will inevitably decline if all CSPs go to NAT/PAT.

Cyber bullying disrupted or hacking prevented.
The use of IP address resolution could be the only way to identify suspects in cyber bullying disrupting cyber enabled crimes; for example hacking and cyber bullying.

Other Crime and vulnerable people

CD is already routinely used by law enforcement agencies when investigation crime. IP address resolution, as part of information available from CD, may form part of investigations in other areas. It has been used to solve murders, seize assets but also importantly to help identify threat to life cases where a vulnerable person may intend to take their own life.

The change in the way people communicate has meant that vulnerable people will often 'post' their intentions to harm them self on social media websites. This means being able to identify the unique attributes necessary to answer the question of 'who' in the real world was using an IP address at a given point in time and the location, will enable law enforcement and other emergency services to quickly locate those vulnerable people.

In addition, IP address resolution, as part of information available from CD, may form part of investigations in other areas including lives saved, drugs and firearm seizures, volume crime and asset seizures.

F: One in two out.

F.1 This is out of scope. There is no cost to industry as the expenditure would be reimbursed by HM Government under the cost recovery scheme.

F.2 Benefits and Effect to industry

DRIPA ensures that no public communications provider is either advantaged or disadvantaged by the requirement to retain CD, or the provisions for reimbursement of additional costs. In addition CSPs cannot use or analyse the data which is stored in the retention store for their own business purposes.

Not all CSPs are required to retain data, only those subject to a notice will be required to retain data. The Home Office will enter into discussions with communications companies prior to them being issued with a notice. It is current Government policy to reimburse 100% costs for storage of data required to be retained under legislation. The working arrangements between CSPs and the Government enable reimbursement of the specific costs that the CSPs would not otherwise incur. This does not include opportunity costs.

F.3 Effects on competition

Payments to a CSP may confer a competitive advantage if that CSP used the data it was obliged to generate for its own business or commercial purposes, or if the systems installed to retain and process the data enhanced the CSP's network capability.

DRIPA ensures that no public communications provider is either advantaged or disadvantaged by the requirements to retain CD, or the provisions for reimbursement of additional costs. The notice based approach, prior consultation, and cost recovery mechanisms minimise any implications.

Where there are exceptions currently, benefits to the CSP are assessed and an appropriate adjustment made to the costs reimbursed so there is no competitive advantage to the CSP.

F.4 Small Firms Test

There is potential for small and micro firms to have obligations placed upon them to retain data. However, the notice based approach and the requirement to engage in consultation with any CSP which is to be made subject of a retention notice, will allow the implications and mitigations for any small or micro firms to be discussed. The cost recovery mechanisms will cover any additional costs for those small and micro firms subject to a notice.

G Risks

G.1 Technical challenges

Capabilities to maintain access to communications data will need to be developed incrementally, with regular assessment of costs and benefits. Risks will be further mitigated by continued close partnership with the CSPs, facilitated by legislation that will provide a sound legal basis for CSP data retention.

G.2 Increasing Costs

Costs will be reviewed annually including estimates of optimism bias. The calculation of those costs is in line with HM Treasury Green Book guidance. Optimism bias (OB) is applied in mitigation against projects and programmes being over optimistic about project costs, duration and benefits.

G.3 Business change

A programme to maintain access to CD in a changing technical environment will also require business change in the user community, notably in the police. Staff will need to be provided with the relevant knowledge, skills and training to use internet-derived CD successfully, and law enforcement agencies will need to embed the development of CD capabilities required to do this in their business plans. Both are addressed by the programme to implement the legislation.

G.4 Privacy Issues

There are significant public safety benefits deriving from the proportionate use of CD. There are also risks to privacy. There are, in theory, risks that data may be accessed without the necessary or appropriate approvals; that incorrect data may be returned to a public authority; and that data may be insecurely stored. Under RIPA, there are strict rules on when, and by whom, this data can be accessed and all requests must be assessed in terms of necessity and proportionality. All applications for CD must be authorised by a designated senior officer, at a rank stipulated by Parliament, who is trained in considering the privacy implications of the application.

In each Public Authority, there is a Senior Responsible Officer, who is held accountable for the integrity of the approvals process in that Public Authority. The processing of personal information, including CD, is also regulated by the Data Protection Act. In relation to the safeguards contained in RIPA, the Joint Committee on the Draft Communications Data Bill commented: *"It is our view that the current internal authorisation procedure is the right model."*

In addition to the stringent framework set out in RIPA, DRIPA has further improved safeguards, enhancing our CD retention notice regime and formalising the requirements placed on communications service providers to safeguard this crucial data. It also ensures that data retained purely by virtue of the requirements in the Act cannot be accessed using other information gathering powers with lesser safeguards.

DRIPA places an obligation on CSPs to protect data from accidental destruction, loss, alteration or disclosure and sets out a maximum period of up to 12 months for retention of data by CSPs and a requirement to destroy it at the end of this period.

The Interception of Communications Commissioner will continue to be responsible for oversight of the acquisition of communications data by public authorities. The Information Commissioner has responsibility for oversight relating to the integrity and security of data retained by CSPs and the destruction of such data at the end of the retention period. The availability of the Investigatory Powers Tribunal (IPT) ensures that individuals have a proper avenue of complaint and means of redress if the powers in RIPA have been used unlawfully.

H. Enforcement

Obligations placed on CSPs under this legislation (including obligations to maintain the security of data) can be enforced by civil proceedings brought by the Secretary of State. Independent oversight will be provided by the Interception and Information Commissioner.

I. Summary and Recommendations

The table below outlines the costs and benefits of the proposed changes:

Option	Costs	Benefits
2	£98.9 million (Present value)	N/K

Option 2. This option will address one of the key challenges for law enforcement, in maintaining their capability to investigate crime, by enabling the answering of the question of 'who' in the real world was using an IP address at a given point in time and the attribution of those communications to locations.

J. Implementation

Once new legislation is in force, new CD capabilities will be delivered incrementally based on law enforcement priorities. We will work closely in collaboration with CSPs to ensure necessary CD continues to be available as they deliver new services or switch to new technologies e.g. 4G mobile. New legislation will allow CSPs to deploy solutions to generate and process necessary CD.

K. Monitoring and Evaluation

Programmes enabled by this legislation will be monitored by the Home Office, HM Treasury and the Major Projects Authority in the Cabinet Office. DRIPA has a sunset clause which means that new legislation will have to be introduced to Parliament in December 2016. The case for further legislation will be subject to pre-legislative scrutiny.

L. Feedback

Feedback on the practical impact on those affected will be obtained through the functions of the Interception of Communications Commissioner and the jurisdiction of the Investigatory Powers Tribunal.

M. Specific Impact Tests

M.1 Statutory Equality Duties

A Privacy Impact Assessment will be published when the Bill is introduced.

K. Environmental Impacts

The Bill will increase the volume of CD available to law enforcement and the security and intelligence agencies. It is likely that more storage will be needed to store the additional retained data. The systems necessary to generate, retain and process CD will produce carbon emissions. However, so do the existing systems they will replace. Newer technology is being made more efficient to reduce the impact on the environment. It is recognised that bigger storage systems might result in greater carbon emissions. However, alternative investigative tools that could generate similar outcomes to CD (such as directed surveillance) are likely to have a larger carbon footprint than the solution enabled by the proposed legislation.

Social Impacts

The ECHR memorandum accompanying the Bill provides detailed assessment of ECHR implications. We believe the policy will lead to health and well-being benefits, through the contribution the policy will make to the prevention and detection of crime.

Competition Assessment

We do not believe the policy proposals will directly or indirectly limit the number or range of providers in this market. Compensatory payments to firms to offset the costs of complying with the proposals will ensure no firm is placed at a competitive advantage or disadvantage as a result of this policy change.

We do not believe consumers will switch to overseas providers of services because they perceived the proposals would impact on their privacy.

Justice

We do not believe the policy will have a significant overall impact on the courts, tribunals, prisons and probation, legal aid, prosecuting bodies and judiciary.

By providing a capability that maintains the ability of law enforcement to investigate crime, means that the same people currently committing crimes, who are identified through the use of CD, will continue to be arrested and prosecuted. The proposed policy will also improve the evidence base and efficiency of investigations before cases come to court. It will enable early identification of those who are of no interest to the investigation and thereby saving on court time or the time that people may be held on bail pending the outcome of an investigation.

Maintaining the ability of the police and others to use CD mainly in the context of criminal investigations and threat to life cases will result in more successful prosecutions than would otherwise be the case unless more costly and intrusive investigative techniques were used to plug the gap.