Title: COMMUNICATIONS DATA LEGISLATION **IA No:** HO 0073 **Lead department or agency:** Home Office **Other departments or agencies:** Law Enforcement, Security and Intelligence agencies	**Impact Assessment (IA)** **Date:** 11/05/2012 **Stage:** Final **Source of intervention:** Domestic **Type of measure:** Primary legislation **Contact for enquiries**: DraftCommsDataBill@homeoffice.x.gsi.gov.uk

Summary: Intervention and Options

RPC Opinion: Amber

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**
£ 3.8bn	£m	Nil	Yes	Zero Net Cost

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

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 serious organised crime investigations 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 communications have moved from fixed line telephones to mobiles and the internet. 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 this legislation is to maintain the capability of Public Authorities currently designated under the Regulation of Investigatory Powers Act (RIPA) to get access to communications data. This requires that:

- Communications data from communications services now in common public use continues to be available to Public Authorities;
- Systems are in place ensure the secure, reliable and effective handling and processing of communication data in accordance with lawful requests;
- Safeguards are in place to protect data at all times and to ensure that requests for data are necessary and proportionate.

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

Option 1: No legislation – there is limited scope under existing legislation to address the current gap in available communications data; at best work can continue (as it does at present) to ensure that best use is made of data already available.

Option 2: With legislation – new legislation provides for the legal retention by industry of a wide range of communications data (reflecting the number of services now available) and therefore effectively closes a capability gap which exists (and is growing) at present.

Option 2 is the preferred option and reflects a Government commitment in the Strategic Defence and Security Review to maintain communications data capability.
A variant on proposed legislation - for Government (not industry) to retain more communications data for use by policing and others - has been rejected: a centralised database would change the current framework for the acquisition of communications data and raise fundamental privacy issues.

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:** 5/2017

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

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: Sustainable CD approach

FULL ECONOMIC ASSESSMENT

Price Base Year 2011	PV Base Year 2011	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: £3.2bn	**High: £4.4bn**	**Best Estimate: £3.8bn**

COSTS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	Optional		Optional	**Optional**
High	Optional		Optional	**Optional**
Best Estimate				**£1.8bn**

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

The key costs relate to investment in infrastructure to support the retention and storage of data by Communications Service Providers and the secure and reliable transmission of data to Public Authorities subject to greater safeguards and closer oversight. There will also be some additional burden placed on the Interception and Information Commissioners.

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

Possible intrusions into privacy have not been monetised because we have not been able to determine a relevant unit cost. We are aware of work being carried out on behalf of the European Commission which will establish some relevant unit costs but this is not yet complete.

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

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

There will be direct financial benefits deriving from this programme due to the support that communications data will provide to investigations into financial crimes and investigations leading to the seizure of criminal assets. There are also existing accepted ways of attributing a financial value to other events, notably loss of life, which can be prevented by the use of communications data in a criminal or threat to life investigation. These events also include: threats to the safety and security of children and continued trafficking of drugs. Use of communications data in both investigation and prosecution can provide savings for Public Authorities;, we also expect that the proposed legislation will make the process of obtaining communications data more effective, efficient and secure..

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

Communications data is used in a wide range of other criminal investigations and prosecutions, including investigations into murder and terrorism and is an essential tool in maintaining current rates of prosecution and convictions.

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

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

- Non delivery of capability;
- Potential reduction of funding;
- Technical challenges;
- Privacy intrusion; and
- Increased workload for the Interception and Information Commissioners.

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m: Nil			In scope of OIOO?	Measure qualifies as
Costs: £859m	**Benefits:** £859m	**Net:** Nil	Yes	Zero net cost

Evidence Base (for summary sheets)

A. Strategic Overview

A.1 Background

Communications Data

Communications data is information about a communication and is defined in the Acquisition and Disclosure of Communications Data Code of Practice, approved by Parliament in 2007[1].

Communications data is legally distinct from a communication's content (for example the text of an e mail or a telephone conversation). Under UK law the content of a communication can only be lawfully 'intercepted' under a warrant issued personally by the Secretary of State and in certain other very limited circumstances set out in Chapter 1 of Part 1 of RIPA. Interception cannot be authorised by using the powers and procedures which are particular to communications data.

The ability of the law enforcement, security and intelligence agencies to obtain communications data is vital to public safety and national security. Communications data is used during investigations regarding national security, organised and volume crime where it very often enables the police and others to identify members of a criminal network. It is fundamental to effective policing at all levels and is used as evidence in courts.

Communications data has played a significant role in every major Security Service counter terrorist operation over the last decade.

Increasingly, the police and others are unable to get access to communications data; some data is no longer retained by Communication Service Providers (CSPs) for business reasons; some CSPs offering services in this country are based overseas. Legislation which currently provides a legal basis for the retention and storage by CSPs of communications data (see below) did not envisage recent developments in communications technology or usage and no longer provides an adequate legal basis for a communications data regime.

The Government is introducing for pre-legislative scrutiny, proposals to enable a programme of work to maintain the capability of law enforcement and other agencies to access communications data. This Impact Assessment (IA) examines these proposals.

Existing legal framework

The EU Data Retention Directive (2006) (EUDRD) requires UK communication providers to retain certain specified types of telephony and internet related communications data which is generated or processed in connection with their business for 12 months. The EU directive was transposed into UK law by the Data Retention (EC Directive) Regulations 2009. In addition, certain data is retained in accordance with a voluntary code of practice on data retention, under the Anti

[1] Acquisition and Disclosure of Communications Data Code of Practice Pursuant to section 71 of the Regulation of Powers Act 2000 (TSO July 2007)

Terrorism, Crime and Security Act 2001. This voluntary code, produced following extensive consultation with industry, enabled CSPs to retain certain communications data they held for business reasons for longer than they would otherwise have done. Many elements of the voluntary code were then used as the basis for the mandatory obligations in the Data Retention Directive.

Access to communications data by law enforcement and the security and intelligence agencies (and other relevant public authorities) is primarily regulated by the Regulation of Investigatory Powers Act (RIPA 2000). RIPA places strict rules on when, and by whom, data can be obtained and provides authorities with a framework for acquiring communications data which is consistent and compatible with the European Convention on Human Rights (ECHR).

The processing of personal information, including communications data, and the storage of personal data by industry is also subject to the Data Protection Act (DPA) 1998.

A.2 Groups Affected

The groups affected by this legislation will be:

- Communications Service Providers (CSPs);
- Law Enforcement Agencies (LEAs);
- Security and Intelligence Agencies (SIAs);
- Other designated Public Authorities;
- 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.3 Consultation

The following Government departments and public bodies have been consulted:

- Association of Chief Police Officers (ACPO)
- Association of Chief Police Officers Scotland (ACPOS)
- Cabinet Office
- Child Exploitation and Online Protection Centre (CEOP)
- Crown Prosecution Service
- Foreign and Commonwealth Office
- GCHQ
- Her Majesty's Revenue and Customs (HMRC)
- Metropolitan Police Service
- Ministry of Justice
- Northern Ireland Office
- Police Federation of England and Wales
- Police Service for Northern Ireland
- Security Service
- Serious Organised Crime Agency

All Government Departments were consulted regarding the restriction of powers to acquire communications data.

B. Rationale

As ways of communicating have changed and increased so the capability of the police and others to obtain access to communications data has been eroded.

There are two specific problems:

- Current legislation does not require CSPs in the UK to generate and/or retain all types of communications data from all the services they provide,
- There has been a significant uptake in the use of new communications services (e.g. webmail, social networking and gaming services) which are almost entirely provided by companies located overseas. Many companies offering newer forms of communications services do not store communications data in the UK and are not legally required to do so. They have no commercial database in this country which relevant public authorities may access under existing legislation. UK network providers (which are used by overseas providers to carry their services to domestic customers) have no business need to retain this data and no legal obligation to do so.

Under Part 1 of the Bill, 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 e.g. data relating to new or innovative communications services; retain this data safely and securely; and hold the data a way that facilitates efficient disclosure of this data to public authorities. Notices will ensure sufficient communications data (including historic communications data) is available for specific communication services, especially certain Internet-based services, from particular CSPs. CSPs who may be affected will be consulted before a notice is issued. CSPs will also be entitled to refer the notice to the joint industry-public authority Technical Advisory Board (TAB) who will consider representations about technical and financial consequences of the notice for them.

Part 2 of the Bill will provide a lawful basis for the Secretary of State to establish additional automated systems to facilitate the efficient and secure obtaining of communications data by Public Authorities in an increasingly complex communications environment.
Part 3 of the Bill will enable contributions to be made towards the costs incurred by CSPs in complying with these new obligations.

RIPA places strict rules on when, and by whom, access can be obtained to communications data retained and stored by industry. The proposed legislation would preserve the essential elements of this framework, and makes several improvements designed to increase safeguards and enhance the compatibility of the statutory framework as a whole with the European Convention on Human Rights (ECHR).

New safeguards will include:

- Requirements to ensure the integrity and security of stored communications data (for example to protect against accidental loss or unauthorised disclosure);
- A specified maximum retention period of 12 months and a requirement to then permanently destroy the data;
- Additional oversight for the Information Commissioner relating to the integrity and security of data retained by CSPs and the destruction of such data at the end of the retention period.
- Automated systems to obtain, process and filter communications data so only data relevant to a specific enquiry will be disclosed to a Public Authority. Authoritative records will be created that can be audited regularly.
- An explicit statement in the Bill that collection of content is not permitted by the new legislation. The Interception of Communications Commissioner will have new responsibilities to oversee the testing and audit of systems to distinguish content of communications from the 'who, how when and where' of a communication.

The new legislation therefore maintains the scrutiny, approval and oversight roles of Parliament, Interception of Communications and Information Commissioners, the Investigatory Powers Tribunal and Technical Advisory Board (established under RIPA).

C. Objectives

The objective of this legislation is to maintain the capability of the designated authorities, notably the police, to have access to communications data, primarily in the context of a criminal and/or a threat to life investigation.

D. Options

The following options have been considered:

Option 1: no new legislation.

Under this option the acquisition of communications data by UK law enforcement and other agencies would continue to be based on existing legal provisions. There would be continued but limited investment in projects to make more effective use of existing communications data, recognising that the existing capability gap (between data requested and data available) would continue to grow.

This option would mean:

- Continued degradation of the lawful capability to acquire communications data;
- Growing disruption to current techniques used for the investigation of crimes and other threat to life situations (e.g. missing persons);
- A reduction in rates of crime detection and criminal prosecution.

Option 2: New legislation enables a programme of activity to maintain access to communications data.

Proposed new legislation will be introduced that seeks to maintain capabilities to acquire and lawfully use communications data acquired by CSPs by:

- Introducing new requirements on CSPs to generate, obtain, process and retain communications data, including data beyond their business need;
- Providing for new arrangements to facilitate the secure, efficient and effective transmission of communications data to public authorities; and
- Providing for payments to be made to CSPs in respect of costs incurred in complying with the new legislation.

This is the preferred option as it delivers the highest level of benefit to operational stakeholders, and with the best cost-benefit ratio is also the most cost effective. It is capable of adapting to evolving technologies and useage of communications services.

E. Appraisal (Costs and Benefits Best Estimates)

E.1 General Assumptions and Data

The communications industry, communications technology and communications usage are all changing quickly. Programmes to maintain access to communications data must proceed with caution to avoid being overtaken by events. Estimated costs (and benefits) may therefore also change and will be subject to regular review.

The costs and benefits used in this assessment were generated in the process of building the most recent programme business case that was approved by the Home Office and HM Treasury in June 2011. The business case was based on the following assumptions:

- Communications traffic continues to grow year on year;
- The total volume of internet traffic increases by a factor of ten over the 10 year period;
- CSPs are required to retain communications data for up to 12 months; and
- Data storage costs continue to decrease by 25% per annum.

The business case followed the HMT Green Book methodology.

E.2 OPTION 2 – Legislative changes regarding Communications Data

Costs

Costs include the provision of equipment within CSPs to collect and retain data and interfaces to permit transmission of this information to requesting authorities. In addition, CSPs are reimbursed for the costs of processing requests to supply data to relevant public authorities.

The main cost categories are as follows:

- **Current work** with major UK telecommunication operators to implement data retention solutions resulting from the EUDRD;
- **Operational enhancements** undertaken within the limits of current legislation with a particular focus on training investigators;
- **Risk reduction** to help identify the technical and operational challenges in implementing a long-term solution; and
- **Strategic work** to develop and implement the preferred option (2) to address the challenge presented by new and emerging technologies, requiring new legislation.

Total discounted economic costs over 10 years starting from 2011/12 are estimated to be £1.8 billion. This represents the cost of the programme without allowing for inflation, Value Added Tax and depreciation. This is consistent with HM Treasury Green Book guidance.

Alternative methods of investigation, such as directed surveillance and undercover officers, cost significantly more than communications data, do not provide the same level of benefit and are very often more intrusive. The proposed *10 year* investment in communications data capabilities of £1.8 compares with an annual cost for policing alone of £14 billion.

Benefits

Over the ten year period to 2020/21 expected benefits from addressing the decline in the proportion of communications data available to the police and others are estimated to be £5.0 – £6.2 billion. These benefits are assessed by operational stakeholders and, using a model validated by HM Treasury, translated into economic values. The assessment takes into account an analysis of criminal behaviours by the Serious and Organised Crime Agency and an analysis of the future communications market based on OFCOM and other market sources. The largest categories of benefits are direct financial benefits arising mainly from preventing revenue loss through tax fraud and facilitating the seizure of criminal assets. Values for benefits for example from lives saved and children safeguarded are derived from standard estimates by Home Office economists[1]. Like costs, benefits are subject to regular review.

[1] Home Office Research Report 217: The economic and social costs of crime against individuals and households 2003/2004 Home Office Online Report 30/05, and were adjusted to 2010/11 prices.

The estimate of benefits does not include benefits that cannot be monetised. These include illicit drugs seized, successful murder convictions and the prevention of terrorism.

E.3 One–in-One-Out (OIOO)

Costs to Industry (INs)

The additional costs to the private sector relate to the investment in capabilities required by CSPs to implement suitable systems to capture, retain and transmit data. These are estimated at £859m over ten years.

These costs include the costs of retaining and processing additional management information to allow the Information and Interception of Communications Commissioners to oversee the use of communications data effectively, and operating and operational costs relating to the new systems, such as staff training for CSPs and CSP engagement in staff training for public authorities. The ten year figure includes £170m for the extension of existing legislative requirements under the EU Data Retention Directive (EUDRD) which mandates some retention of specific IP data. There are separate costs associated with individual requests for communications data drawn from systems in place, which are estimated by CSPs on an individual basis.

The proposed legislation could distort the UK telecommunications market if UK consumers switched to overseas providers of services because they perceived that the legislation would impact on their privacy. The majority of overseas providers, however, operate under similar, if not more intrusive legal regimes, without the rigorous safeguards provided by the proposed UK legislation. We therefore believe that there is unlikely to be any significant or lasting distortion of the market.

Benefits to Industry (OUTs)

The costs to the private sector of complying with its legal requirements under the proposed measure will be defrayed by the Secretary of State. The benefits are therefore estimated to be £859m.

The costs associated with individual data requests are currently defrayed by a transfer from the designated public authorities concerned to CSPs concerned.

The existing legislation results in a burden as a result of complying with the working arrangements between CSPs and the Government. Today the Home Office works closely with CSPs to ensure that appropriate systems are in place so the designated Public Authorities can efficiently obtain the communications data needed to carry out investigations. Agreeing the nature of those systems (and the costs to be refunded for them) imposes an overhead on all parties which is not refunded for CSPs. Negotiations can be technically detailed and burdensome.

The proposed legislation provides a more clearly defined legal basis for the extent of the systems which may be agreed with CSPs. It is therefore expected to reduce the amount of negotiation which is necessary and thus reduce the overhead imposed on CSPs.

NET

The policy is therefore expected to have minimal net impact on the private sector overall.

F. Risks

OPTION 2 – Legislative change regarding Communications Data

Technical challenges

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 evolving internet behaviour (an analogous example is virus detection software that develops in tandem with new threats). Risks will be further mitigated by close partnership with the CSPs, facilitated by legislation which will provide a sound legal basis for CSP data retention and storage.

Increasing costs

Technical complexity can increase projected costs. Actions set out above to mitigate technical challenge will also address the risks of a costs overrun. There will be close engagement with industry suppliers and CSPs. In addition, in line with the HM Treasury 'Green Book', 'optimism bias' has been included, which allows for the tendency for early estimates of the cost of major programmes to be understated.

Business change

A programme to maintain access to communications data in a changing technical environment will also require business change in the user community, notably in the police. There will be changes in the type of communications data that is used and in the ways in which it has to be interpreted.

Privacy Issues

There are significant public safety benefits deriving from the proportionate use of communications data. But 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 Public Authority; and that data may be insecurely stored. These and other privacy issues are considered

in detail in a separate Privacy Impact Assessment. Mitigation of these risks is provided by existing and new safeguards.

Access to communications data is currently regulated by the Regulation of Investigatory Powers Act (RIPA), which places strict rules on when, and by whom, this data can be obtained and stipulates that requests must be assessed in terms of necessity and proportionality. All applications for communications data 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. These protections will be replicated by Part 2 of the Bill (which will replace the current RIPA framework for acquiring communications data). The processing of personal information, including communications data, is also regulated by the Data Protection Act.

Legislation will only allow the communications data which is retained by Communications Service Providers to be used for permitted purposes (i.e. those set out by the legislation). The data cannot be accessed by CSPs for their own business purposes. New legislation also places an obligation on CSPs to protect data from accidental destruction, loss, alteration or disclosure.

Consistent with the UKs transposition of the EUDRD, a maximum period of 12 months for retention of data by CSPs and a requirement to destroy it at the end of this period are set out on the face of the Bill.

The Interception of Communications Commissioner will continue to be responsible for oversight of the acquisition of communications data by public authorities. The Information Commissioner will be responsible 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 powers of the Investigatory Powers Tribunal (IPT) will be extended to ensure that individuals have a proper avenue of complaint and independent investigation if they think the powers have been used unlawfully.

In addition to overseeing the acquisition of communications data by public authorities the Interception of Communications Commissioner's duties will keep under review the collection of communications data by CSPs and the transmission of data to public authorities. The Interception of Communications Commissioner will ensure that any equipment CSPs use to generate and process communications data will be adequately tested before operational rollout, regularly audited, and noted defects recorded and handled correctly;

There is some risk of increased workload for the Interception of Communications Commissioner and the Information Commissioner. The Government will continue to ensure that the Interception of Communications Commissioner is resourced in order to be able to meet his statutory responsibilities. The Commissioner reports annually to the Prime Minister on the carrying out of his oversight responsibilities and his report is laid before Parliament and published. We continue to work with the Information Commissioner to ensure ongoing compliance with Data Protection Principles and Data Protection Act.

Potential reduction of funding

While funding has been allocated, there remains a risk of a reduction in funding if macro-economic conditions worsen. Such a reduction would affect operational stakeholders' ability to mitigate capability degradation.

G. 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 of Communications Commissioner and the Information Commissioner.

H. Summary and Recommendations

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

Table H.1 Costs and Benefits

Option	Costs	Benefits
2	2011/12 – 2020/21 £1.8bn	2011/12 – 2020/21 £5,0 - £6,2bn
	Cost to public sector - £1.8 bn Costs to private sector - Nil	Benefits to UK to 2020/21 £5.0-£6.2bn

Source: CCD OBC discounted

Although it requires a high investment, the programme underpinned by Option 2 has been shown to best close the existing capability gap regarding communications data. It performs well in respect of the risks and the technical challenges, both with CSPs and the law enforcement community. In addition, the business change requirements are manageable.

I. Implementation

Once new legislation is in force, new communications data capabilities will be delivered incrementally based on law enforcement priorities. We will work in collaboration with CSPs to ensure necessary communications data continues to be available as they deliver new services or

switch to new technologies e.g. 4G mobile. Over the next 2-4 years new legislation will allow CSPs to deploy solutions to generate and process necessary communications data.

J. Monitoring and Evaluation

Programmes enabled by this legislation will be monitored by the Home Office and H.M Treasury. A benefits realisation plan has been developed in conjunction with stakeholders and will continue to be updated on a yearly basis.

A Post Implementation Review (PIR) Plan will be undertaken five years after implementation of the policy. The PIR will examine the extent to which the implemented regulations have achieved their objectives, assess their costs and benefits and identify whether they are having any unintended consequences.

K. Feedback

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

L. Specific Impact Tests

Statutory Equality Duties

Privacy Impact Assessment

A Privacy Impact Assessment has been published alongside the Bill.

Social Impacts

Human Rights

The ECHR memorandum accompanying the Bill provides a detailed assessment of the ECHR implications.