

Draft Communications Data Bill Privacy Impact Assessment

Purpose

This document is the Privacy Impact Assessment (PIA) for the implementation of proposed communications data legislation contained in the draft Communications Data Bill, which is to undergo pre-legislative scrutiny.

The purpose of this PIA is to:

- consider the privacy impact of the proposed legislation;
- assess whether the capabilities implemented through this proposed legislation will be compliant with the Data Protection Principles (DPP) and the Data Protection Act 1998 (DPA).

DOCUMENT REFERENCES

Ref. No.	Title	Document Reference
1	Information Commissioner's Office (ICO) ' Privacy Assessment Handbook v2.0'.	Available at: www.ico.gov.uk
2	Data Protection Guidance Note	Available at: www.ico.gov.uk
4	REGULATION OF INVESTIGATORY POWERS ACT 2000: Consolidating Orders and Codes of Practice, 2009	Available at: www.homeoffice.gov.uk
5	Report of the Interception of Communications Commissioner for 2009	Available at: www.ipt-uk.com

Table of Contents

1. EXECUTIVE SUMMARY	5
2. THE CASE FOR LEGISLATION.....	5
2.1 Rationale	5
2.2 Strategy	6
2.3 Overview of the proposed legislation	6
3. PRIVACY IMPACT ASSESSMENT: APPROACH	6
3.1 Introduction.....	7
3.2 ICO requirement for a Privacy Enhancing Technologies assessment	7
3.3 Equality Act considerations	7
4. OVERVIEW OF CURRENT AND PLANNED SAFEGUARDS.....	7
5. PRIVACY RISKS	9
5.1 The risk of inappropriate or inaccurate authorisation by a public authority of requests for communications data	9
5.2 The risk of collateral intrusion	11
5.3 The risk that retention of data by CSPs and ISPs will unnecessarily and disproportionately intrude on privacy	13
5.4 The risk of unauthorised use or mishandling of communications data retained by CSPs...	14
5.5 The risk that incorrect data is returned by CSPs.....	15
5.6 The risk that communications data held by CSPs is not appropriately protected.....	16
5.7 The risk that technical systems enabled by the proposed legislation are not appropriately protected	16
5.8 The risk that communications data is not destroyed by CSPs	17
6. PRIVACY IMPACT STATEMENT.....	17
6.1 Data Controllers and Data Processors	17
6.2 Subject Access Requests.....	18
7. RELEVANT LEGISLATION.....	18
ANNEX A: GLOSSARY	20

ANNEX B: TYPES OF COMMUNICATIONS DATA21

ANNEX C: RELEVANT LEGISLATION23

ANNEX D: PRIVACY ENHANCING TECHNOLOGIES (PET) ASSESSMENT25



1. Executive summary

This Privacy Impact Assessment (PIA) follows the approach and guidelines recommended by the Information Commissioner's Office (ICO). It considers the impact on privacy of the proposed communications data legislation: communications data is regarded as personal data as defined by the Information Commissioner.

The PIA identifies the risks to privacy arising from the capabilities that will be enabled by the new legislation and sets out the safeguards, existing and new, intended to address these risks (section 5). The PIA concludes with a Privacy Impact Statement (see section 6).

2. The case for legislation

2.1 Rationale

Communications data has played a role in every major Security Service counter-terrorism operation over the past decade and in 95 per cent of all serious organised crime investigations. It is vital to law enforcement, especially when dealing with organised crime gangs, paedophile rings and terrorist groups. It enables the police to build rapidly an authoritative picture of the activities and contacts of a person who is under investigation. Unlike the content of a communication, communications data can also be used as evidence in court. Further details about the definition and scope of communications data are set out in Annex B.

Many communications have now moved from fixed line telephony to mobile telephones and the internet. The internet has vastly increased the ways and extent to which people can communicate and the amount of generated data; new forms of communication like instant messaging, social networking and multi-player online gaming are now widely used.

As communications have moved to the internet so the ability of the police and other public bodies to get access to communications data has been eroding. There are two particular challenges:

- Current legislation (based on the provisions in the European Data Retention Directive) does not require Communication Service Providers and Internet Service Providers (CSPs and ISPs) in the UK to retain all the communications data from the communications 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. 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.

Inability to get access to communications data is already affecting the ability of the police and others to investigate crime and bring criminals to justice. Unless action is taken the capability gap will grow as a greater proportion of communications data will cease to be available.

Alternative tactical capabilities available to the police and the agencies (including direct surveillance, intrusive surveillance and covert human intelligence sources) offer no like for like alternative to communications data and have a number of disadvantages:

- They do not provide historic evidence or intelligence (e.g. when investigating a crime which has occurred);
- They can be more intrusive than communications data;
- They are significantly more expensive and resource intensive.

2.2 Strategy

The Office of Security and Counter Terrorism (OSCT) in the Home Office is responsible for the strategy to maintain the availability of communications data, primarily for policing. OSCT is responsible for programmes to ensure that data is available under existing legislation, that (subject to the necessary authorisations) it can be quickly and securely transmitted to the police and others and that the police and others are capable of using it in the context of an investigation.

This legislation is a key part of the future strategy to maintain the availability of communications data for the protection of the public and public safety.

The strategy is informed by close engagement with: the users of communications data, notably the police and agencies; and the CSPs and ISPs whose services generate data and whose technology is essential in making data available.

2.3 Overview of the proposed legislation

The proposed legislation will establish an updated framework for the obtaining and retention of communications data by CSPs and for obtaining that data by authorised public authorities.

Under Part 1 of the draft Communications Data 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 in a way that facilitates efficient disclosure of this data to public authorities. Notices will ensure sufficient communications data (including historic communications data) is available, 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 draft Bill provides a lawful basis for the Secretary of State to establish arrangements to facilitate the efficient and secure obtaining of communications data by public authorities whilst protecting privacy. These will facilitate the obtaining of communications data by relevant public authorities, and assist the Designated Senior Officer to determine whether the tests for granting an authorisation are met.

Part 3 of the Bill confers further scrutiny functions on the Interception of Communications Commissioner and the Investigatory Powers Tribunal and removes other statutory powers with weaker safeguards which are currently used by public authorities to acquire communications data. Part 3 will also enable contributions to be made towards the costs incurred by CSPs in complying with these new obligations.

3. Privacy Impact Assessment: approach

3.1 Introduction

This PIA follows the approach and guidelines recommended by the Information Commissioner's Office (ICO). The ICO was fully consulted on this PIA and it reflects their advice. The PIA considers the risks to privacy from the proposed legislation. The PIA has been informed by an ICO questionnaire on compliance with the Data Protection Principles (DPP) and the Data Protection Act 1998 (DPA).

As a public authority the Home Office is subject to the Government's Data Handling Review, which sets a number of mandatory measures *"All departments must conduct Privacy Impact Assessments so that they can be considered as part of the information risk aspect of Gateway Reviews or whilst going through accreditation if no Gateway has been conducted for a particular system"*.

The PIA will be updated and published to take account of the strategy of phased delivery of new capabilities. Some data protection risks will however be more appropriately considered in the CSPs' and public authorities' PIAs because systems will differ between organisations.

CSPs are subject to the Data Protection Act and although there are no statutory obligations on them to produce PIAs they will be strongly encouraged to do so, or provide alternative equivalent assurance.

3.2 ICO requirement for a Privacy Enhancing Technologies assessment

The Information Commissioner's Office has developed an implementation plan for designing privacy protection into projects, following recommendations of the "Privacy by Design" Report (dated 26/11/2008). The ICO's implementation plan, lists privacy specifications to be included in the business case for new systems. The plan also recommends a requirement that systems should incorporate appropriate Privacy Enhancement Technologies (PET), based upon rigorous Privacy Impact Assessments and that privacy needs should be managed throughout the lifetime of a system.

The ICO implementation plan also defines activities for developing privacy standards and promoting PETs. The Home Office Communications Capability Development Programme will undertake the required activities when implementing new systems enabled by the proposed legislation. An assessment and applicable actions, taken from the implementation plan are included in Annex D: Privacy enhancing technologies (PET) assessment.

3.3 Equality Act considerations

The Equality Duty, introduced by the Equality Act 2010 requires public bodies and others carrying out public functions to have due regard to the need to eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act. The public protection and national security issues the proposed communications data legislation seeks to address apply to all UK citizens and those visiting the UK irrespective of age, disability, gender reassignment, pregnancy and maternity, race, religion, sex or sexual orientation and it is not believed that any of these groups will be disproportionately affected by the implementation of the proposed legislation.

4. Overview of current and planned safeguards

The Regulation of Investigatory Powers Act (RIPA) 2000 (part 1 chapter 2), provides a regulatory framework which ensures that public authority access to communications data is ECHR compliant. It includes the following key safeguards:

- Communications data may only be acquired by public authorities that have been approved by Parliament under RIPA;
- Communications data may only be acquired for specific purposes set out in RIPA;
- Data is obtained on a case by case basis and must be authorised by a senior officer in a public authority at a rank stipulated by Parliament;
- The authorising officer is required to consider in detail whether an application for communications data is necessary and proportionate;
- Public authorities have different levels of access to the three types of communications data (Annex B refers). Local authorities have significantly less access than the police and are confined to subscriber and some service data. Following the Protection of Freedoms Act 2012, local authorities will be required obtain the approval of a magistrate before they can access communications data
- The Interception of Communications Commissioner provides oversight of the acquisition of communications data by public authorities, including through inspections of Public Authorities. He provides a (published) annual report to the Prime Minister.

The framework for obtaining communications data in the new legislation will replace Chapter 2 of Part 1 of RIPA and will sit alongside the Data Retention (EC Directive) Regulations 2009. The legislation will in addition contain the following new safeguards:

- Other statutory powers with weaker safeguards which are currently used by public authorities to acquire communications data will be removed...
- In line with the Data Retention (EC Directive) Regulations 2009 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. A relevant public authority can request to retain particular communications data for longer for the purposes of legal proceedings
- There will be specific statutory requirements on CSPs holding data as a result of the proposals, to protect the data against accidental or unlawful destruction, accidental loss and unauthorised access or disclosure.
- It will be the role of the Information Commissioner to keep under review the operation of the provisions relating to the security of retained communications data and their destruction after 12 months.
- The role of the Interception of Communications Commissioner will be extended to oversee the obtaining (including by collection and generation) of communications data by CSPs. This will include oversight of testing, regular auditing and inspections.
- The role of the independent Investigatory Powers Tribunal (made up of senior judicial figures) will be extended to cover the new provisions, ensuring that individuals have a proper avenue of complaint and independent investigation if they think the powers have been used unlawfully.

The proposed legislation would enable development of new, automated systems to filter data from CSPs so that only the relevant, filtered data necessary to answer a particular request is disclosed to public authorities. These systems would also create authoritative records regarding the movement of data.

The Interception of Communications Commissioner will ensure that:

- Public authority communication data requests are correctly approved and a Single Point of Contact (SPOC)¹ and Designated Senior Officer² in the public authority have been trained/certified to necessary levels; any equipment CSPs use to generate and process communications data is adequately tested before operational rollout, regularly audited, and noted defects recorded and handled correctly;
- The new systems will be regularly audited to ensure that any CSP that disclose more communications data than is required in a particular request (and other errors) record, report and handle these errors correctly.

5. Privacy Risks

This section considers the impact on to privacy from current and proposed communications data regime and corresponding safeguards. Some of these safeguards are current; others will be new under the proposed legislation.

5.1 The risk of inappropriate or inaccurate authorisation by a public authority of requests for communications data

There is a risk that a public authority incorrectly authorises a request to obtain communications data or that a request is made which is inaccurate. These errors could cause unnecessary or disproportionate intrusion.

• Existing safeguards - Regulation of Investigatory Powers Act 2000 (RIPA).

Lawful purpose. Part I Chapter II of the RIPA sets out a strict statutory regime regulating how public authorities can obtain communications data. It limits the purposes for which data can be acquired from a CSP by the police and other Public Authorities. Communications data can be obtained in particular cases if it is:

- In the interest of national security;
- For the purpose of preventing or detecting crime or preventing disorder;
- In the interests of the economic well-being of the UK;
- In the interests of public safety;
- For the purpose of protecting public health;
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- For the purpose in an emergency of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person physical or mental health;
- To assist investigations into alleged miscarriages of justice;

¹ An accredited individual or a group of accredited individuals, trained to facilitate lawful acquisition of CD and effective co-operation between a public authority and CSPs

² A person holding a prescribed office in a relevant Public Authority who considers the application and records his/her considerations at the time.

- For the purpose of assisting in identifying any person who has died other than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime;
- Obtaining information about the next of kin or other connected persons of such a person or about the reason for their death or condition.

Applications for communications data have to pass through a number of separate stages of approval:

- The applicant in the public authority sets out in an application the requirement for communications data, the data which is needed in relation to which individual, together with an assessment of why the request is necessary and proportionate; the application is considered by a senior officer, known as the designated person;
- The Single Point of Contact is an expert in the use of communications data (accredited by the Association of Chief Police Officers (ACPO) Data Communications Group) in the same public authority, trained to understand technical aspects of communications data, and the potential privacy impact of data applications. The SPoC will advise the applicant prior to the application and later provide advice to the designated person. They will often be independent of the investigation, to ensure that they provide impartial advice.
- The designated person is a senior officer in the public authority, at a rank stipulated by Parliament, trained in considering the impact on human rights of acquisition. It is their responsibility to assess the necessity and proportionality of the application, and authorise or refuse to authorise the acquisition of communications data. They may seek advice from the SPoC on the level of the collateral intrusion of the activity (for more details on collateral intrusion see 5.2 below) outlined in the application, or on how an application might be tightly drawn. Good practice under the Code of Practice³ dictates they should be independent of the investigation, but the law requires them to be a member of the same police force.
- The process is overseen by the Senior Responsible Officer, who is held accountable for the integrity of the process. Once approved, the Single Point of Contact acquires the data and passes it to the applicant.

Necessity and proportionality. The RIPA regime was established to ensure that public authority use of surveillance powers and access to communications data is compatible with the European Convention on Human Rights, particularly Article 8. RIPA requires public authorities to satisfy tests of necessity, proportionality and legitimate aim before obtaining communications data.

The authorising officer must consider whether obtaining communications data is necessary for a statutory purpose. They must consider whether the acquisition of communications data is proportionate to the objective (i.e. the objective of the investigation which is underway). This explicit requirement means that the officer authorising a communications data request must balance the importance of the specific benefit of that request against any intrusion into privacy.

The authorisation will only be given if the senior authorising officer considers that obtaining the communications data would be both necessary for a statutory purpose and proportionate to what the investigation is seeking to achieve.

³ Acquisition and Disclosure of Communications Data Code of Practice Pursuant to section 71 of the Regulation of Powers Act 2000 (TSO July 2007)

Independent Oversight. The Interception of Communications Commissioner provides independent oversight of the process for requesting, authorising and obtaining access to communications data. The Interception of Communications Commissioner must have previously been a senior judicial figure; currently the post is held by the Right Honourable Sir Paul Kennedy.

The Commissioner has a team of inspectors who ensure that public authorities fulfil the strict requirements of the law set out in RIPA and the statutory Code of Practice which supports this. Inspections of public authorities take place throughout the year and the Commissioner provides a report annually to the Prime Minister which is laid before Parliament.

These inspections look at a proportion of communications data requests made by public authorities and at disclosures made by CSPs. To identify any unauthorised disclosures the Intercept of Communications Commissioner's Office (IOCCO) selects a sample of communications data disclosures made by a CSP and then inspects the authorisation documents at the requesting authority. More information on this can be found in the IOCCO Annual Reports www.ipt-uk.com

Public authorities are required to report any errors which result in wrongful disclosure of communications data to the IOCCO. The number of errors reported is monitored and this information helps the Commissioner to decide which public authorities to inspect.

The IOCCO report 2010 (the latest available at the time of drafting this assessment) notes 640 errors during the reporting year of which "approximately 82% are attributable to Public Authorities and the remaining 18% to CSPs and ISPs". During this period 552,550 requests for communications data were made.

The report states that:

"Overall ... the error rate is still low and indeed minute (0.3%) when compared to the number of requests that were made by all Public Authorities during the course of the reporting year..... More police forces and CSPs are introducing automated systems to manage their requirements for communications data and these will reduce the number of keying errors which occur. It is inevitable that some mistakes will be made, especially when Public Authorities are dealing with large volumes of communications data in complex investigations."

The IOCCO can direct public authorities to take remedial action to improve their process and lower the number of errors they generate.

The Investigatory Powers Tribunal (IPT) was set up by RIPA to provide for review by a judicial body of conduct by Public Authorities under RIPA, including in relation to the obtaining of communications data. The Tribunal has the power to investigate complaints and if they are upheld can quash authorisations, order the destruction of records and award financial compensation.

5.2 The risk of collateral intrusion

When communications data is obtained by a public authority from a CSP or ISP there is a risk that it includes the personal data of individuals who subsequent analysis shows are not connected with the relevant investigation and not implicated in any crime. This is known as 'collateral intrusion'. The subject of the investigation may for example have made a number of calls just before a crime occurred in which the subject appears to be implicated. Subscriber details for all of these numbers may be obtained in order to establish if there was a criminal connection between the calls and the crime itself. Investigation may determine that there was no such connection.

Collateral intrusion is not unique to work with communications data. In any criminal investigation people may be interviewed who subsequent research demonstrates are innocent. Indeed, some intrusion is almost inevitable in an investigation no matter what methods are used (e.g. door to door enquiries, appeals to the public for information, directed or intrusive surveillance). There are safeguards in place to minimise the impact on privacy, to ensure that collateral intrusion is understood and evaluated, and to record if it happens in error. These safeguards are set out below.

- **Existing safeguards:**

The authorisation process for communications data requests is a principal safeguard. All requests for communications data are carefully considered. A requesting officer documents the extent of collateral intrusion that may arise if the data is obtained. The authorising officer must independently confirm that obtaining what may be collateral data will be proportionate to the objective of the investigation. The officer must compare the extent of intrusion with the seriousness of the particular crime being investigated. Requests which may cause a high level of collateral intrusion will need to demonstrate a proportionate requirement to obtain the communications data before authorisation is given: the authorisation process is discussed more fully in section 5.1.

- **New safeguards**

Processing and filtering of data

Some aspects of internet based communications impact on the acquisition of communications data by public authorities. For example, the technology used to operate internet and mobile services, and collaboration between numerous CSPs and ISPs may mean that communications data regarding a single communication is no longer retained in a single place. This fragmentation of data makes it harder to obtain and aggregate all of the communications data the public authority may need to answer a specific question.

The systems proposed in this legislation to identify the key facts around a communication from fragmented data themselves provide further safeguards against collateral intrusion.

The “Request Filter” enabled by the proposed legislation will significantly reduce intrusion by:

- informing a public authority of the communications data which is available to resolve a specific enquiry; and enable that authority to judge whether in that context the request for data remains necessary and proportionate;
- obtaining, processing and filtering communications data needed to resolve more complex requests so that only data specified in the authorisation which identifies the key facts is passed to a public authority; and
- protecting privacy and minimising interference with the rights of telecommunications users by processing the data without human intervention, and destroying any communications data found to be irrelevant to the investigation.

The Request Filter need only be used in those cases where answering questions regarding the “who, how, when and where” for a single communication requires analysis of fragmented communications data and when use of the Filter is both necessary and proportionate.

Parliament will designate which public authorities will be permitted to use the Request Filter. Parliament will also set out the minimum grade of the Designated Senior Officer within each police force or Agency permitted to authorise the use of the processing and filtering functions in particular investigations.

The operation of the Request Filter will be at one remove from the police, law enforcement or security agency conducting the investigation, minimising any interference with the privacy of those whose data is processed and disclosed. Only the filtered data relevant to the investigation is disclosed to the requesting agency. Once the filter has provided the answer to the question, all the data relating to the request will be destroyed by the filter in such a way that it can never be retrieved.

The Request Filter will also provide the Designated Senior Officer with assistance in determining whether the tests for granting an authorisation are met.

5.3 The risk that retention of data by CSPs and ISPs will unnecessarily and disproportionately intrude on privacy

It is in the business interests of CSPs to maintain the quality of the data they use and, with respect to personal data such as communications data, the data protection principles in the Data Protection Act 1998 require them to do so. Testing regimes ensure that only valid and accurate communications data is retained. In addition, existing and proposed legislation provide substantive safeguards.

Collection of communication content is very intrusive. It is explicit in the proposed legislation that the collection of content cannot be authorised under the legislation. Any attempt to create a system that bypasses the existing legal framework for interception would be unlawful.

- **Existing safeguards:**

Anti Terrorism, Crime and Security Act 2001 (ATCSA) and the EU Data Retention Directive (EUDRD). Current legislation requires communications data to be retained by a CSP when the CSP has a business reason to do so. Legislation relevant to data retention includes the Data Retention Regulations (EC Directive) 2009 (“Data Retention Regulations”) and the Anti-Terrorism, Crime and Security Act 2001 (ATCSA).

In the UK, the ATCSA and the Data Retention Regulations limit the retention period for communications data held by CSPs to 12 months. This timeframe was agreed by Parliament to meet the operational needs of the security, intelligence and law enforcement agencies while ensuring levels of data stored remained appropriate and proportionate. CSPs must delete the data at the end of the retention period in such a way as to make access to that data impossible. The Data Retention Regulations requires CSPs to ensure the quality and security of retained data and to guard against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure of retained data.

It is the duty of the Information Commissioner, as the Supervisory Authority designated for the purposes of article 9 of the Data Retention Directive to monitor how these regulations are applied with respect to the security of stored data. The Regulations are enforceable by civil proceedings by the Secretary of State for an injunction, or for the specific performance of a statutory duty under Section 45 of the Court of Session Act 1988.

Data Protection Act (1998). The Data Protection Act (1998) provides safeguards with respect to data retention. The Act gives the Information Commissioner’s Office (ICO) powers which help protect personal data including communications data. The ICO can:

- Conduct assessments to check organisations are complying with the DPA;
- Serve information notices requiring organisations to provide the ICO with specified information within a certain time period;

- Serve enforcement notices and 'stop now' orders where there has been a breach of the DPA, requiring organisation to take specified steps to ensure they comply with the law;
- Prosecute those who commit criminal offences under the act;
- Report to Parliament on data protection issues of concern; and
- Serve notices requiring organisation to pay up to £500,000 for serious breaches of the DPA.

Under the DPA it is a criminal offence to knowingly or recklessly obtain, disclose or procure the disclosure of personal information without the consent of the data controller. An employee of a public authority or a CSP would commit such an offence if they illegally obtained communications data. It is also an offence to sell or offer to sell illegally obtained personal information.

RIPA framework for interception of communications and associated offences.

Under UK law the content of a communication can only be lawfully intercepted under a warrant issued by the Secretary of State and in certain other very limited circumstances set out in Chapter 1 of Part 1 of RIPA. Interception warrants ensure that the authorised interception is necessary and proportionate and there are extensive statutory protections in relation to the issuing, exercising and oversight of such warrants; RIPA includes an offence for the unlawful interception of communications which carries a term of imprisonment of up to two years.

- **New safeguards:**

Destruction of data beyond the mandated retention period. The proposed legislation requires a CSP to destroy communications data held under the legislation if the retention of the data is no longer authorised by law, in such a way that the data can never be retrieved. The benchmark for implementing this would be the HMG Security Policy Framework and industry Information Assurance standards, for example Information Security Standard (ISO) 27001.

Interception of Communications Commissioner. The new legislation extends the Commissioner's oversight functions to include the obtaining of communications data by CSPs, and testing, regular audit and inspections of the equipment used to collect, store and transfer data. The automated systems enabled by legislation (see section 5.2) will provide more accurate and complete records for this purpose.

5.4 The risk of unauthorised use or mishandling of communications data retained by CSPs

There is a risk that CSPs could use without authorisation or otherwise mishandle the communications data they retain under ATCSA, EU DRD, or the ECHR. It is possible, for example, that data on customers might be lost or misused or that data held under the new legislation might be exploited for business purposes.

- **Existing safeguards**

A set of physical, procedural and technical safeguards exist to prevent unauthorised access to systems in CSPs. Access controls provide users with rights and/or privileges to access and perform functions. Controls should enable authorised users to access the minimum necessary

information to perform their roles. Access controls will include, but not be limited to, unique user identification, automatic logoff and encryption/decryption of credentials and requests.

Computer Misuse Act 1980. Someone who knowingly accesses a computer system that they are not authorised to access in order to obtain or disclose communications data may commit an offence under the Computer Misuse Act 1990. Offences under this Act can carry a term of imprisonment up to two years.

Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (PECR). The ICO has the power to audit the measures taken by CSPs to safeguard personal data. The powers under the PECR only allow the ICO to audit security measures and do not cover the power to audit retention of information (although they do allow the ICO to audit measures taken to ensure personal data is not being unlawfully processed). The ICO will not undertake audits under powers in the amended PECR until they have consulted with CSPs. This consultation is now running and is open until 18th June 2012.

- **New safeguards**

Requirements on CSPs. The proposed legislation sets out that a CSP cannot make use of data collected under the new proposals except in accordance with the provisions of Part 2 of the proposed legislation (i.e. where the data has been requested by a public authority) or for other lawful purpose (e.g. as a result of a Court Order). The draft Bill also requires CSPs to put in place security systems (including management checks and controls) governing access to the data in order to protect against any disclosure not in accordance with the proposed legislation or other lawful purpose. The likelihood of data being lost or mishandled should be reduced by ensuring data protection principles are built into the requirements for implementing the automated system.

Information Commissioner. Under the new legislation the Information Commissioner will have additional oversight duties relating to the integrity and security of data retained by CSPs and the destruction of such data at the end of the retention period. Currently, the Information Commissioner is responsible for oversight of CSP data retained under the EUDRD. This will be extended to include the additional data retained under new legislation.

The Investigatory Powers Tribunal (IPT) will have jurisdiction to entertain claims or complaints (whether brought under the Human Rights Act or otherwise) in relation to conduct by CSPs under the new legislation.

5.5 The risk that incorrect data is returned by CSPs

An error (such as incorrect transcription of a phone number) may occur at the CSP leading to the return of incorrect data.

- **New safeguards**

Better accountability through audit trails and logs. Automated systems provided for in the proposed legislation will provide audit records, independent of public authorities and CSPs, indicating what requests have been submitted by public authorities and how these requests have been addressed. The records will not include personal or other communications data.

These independent records will be a strong deterrent to misuse of communications data, and will assist the IOCCO and ICO in investigating data breaches and errors.

Enhanced consistency and automation of request. Implementation of the proposed Bill will provide a consistent system across public authorities for making requests and ensure a clear interface with CSPs (using defined standards) to streamline the end to end process for requesting, receiving and exploiting communications data. This involves the movement from paper, telephone, fax and semi-automated processes towards fully automated management of obtaining communications data, from initiation of the particular requirement, through review, assessment, approval, acquisition and verification.

5.6 The risk that communications data held by CSPs is not appropriately protected

There is a risk that through a breach of security, communications data held by CSPs could be obtained by an unauthorised third party.

- **New safeguard**

To ensure that privacy is considered at every stage a number of system/implementation PIAs will be conducted, including the evaluation of Privacy Enhancing Technologies (as described in section 3.2).

5.7 The risk that technical systems enabled by the proposed legislation are not appropriately protected

There is a risk that unauthorised persons gain access to the new automated filtering system (see 5.2 above), and thereby unlawfully obtain personal data.

- **New safeguards**

HMG Security Policy Framework accreditation⁴. The new automated filtering systems will be accredited to meet the requirements laid down in the HMG Security Policy Framework (SPF) which sets out the standards, best practices, guidelines and approaches that are required to protect UK Government assets (people, infrastructure and information). The SPF outlines mandatory security requirements and management arrangements to which all Departments and Agencies must adhere. The SPF will apply to the entire infrastructure supporting the collection, retention, processing and obtaining of communications data by Public Authorities.

Access Controls. These will include password, certificate or other secure authentication to access the data processing capability. Access controls will be in place for system applications. Servers will be hosted in a secure location. Protective monitoring will record system activity so that potential security breaches or abnormal activity can be identified, for example attempts at making unauthorised requests.

⁴ The Security Policy Framework is published by the Cabinet Office www.cabinetoffice.gov.uk

5.8 The risk that communications data is not destroyed by CSPs

There is a risk that as equipment is decommissioned and retention periods expires data is not properly destroyed leading to a breach of the DPA.

- **Existing safeguard**

Compliance. The Data Retention (EC Directive) Regulations 2009 provides for the deletion of data at the end of the period of 12 months from the date of the communication subject to any extension for the purpose of legal proceedings.

- **New safeguard**

Destruction of data. New legislation provides for the destruction of communications data at the end of the period of retention (12 months unless extended for the purposes of legal proceedings), in such a way as to make access to the data impossible. The destruction of data must take place within a month of the end of the retention period. The destruction of data will be kept under review by the Information Commissioner.

6. Privacy Impact Statement

This Privacy Impact Assessment has been carried out to assess the risks to privacy posed by the work carried out on the basis of the proposed legislation. It is assessed that implementation of the proposed legislation is capable of being fully compliant with the Data Protection Principles and the Data Protection Act.

6.1 Data Controllers and Data Processors

The data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is or will be processed. The data controller for personal data depends on where it is being stored/processed during the communications data retain/acquire/disclose process.

Under proposed legislation CSPs will be the data controllers until the point where the communications data is disclosed to the public authority or the automated filtering system, when the public authority will be the data controller of the obtained communications data.

6.1.1 Retained data

Retained data is controlled by the CSP.

6.1.2 Automated systems

An automated system will process the communications data on behalf of the public authority in order to:

- minimise the amount of data being disclosed to the requesting public authority;
- minimise the risk of collateral intrusion;
- provide safeguards around proportionality;
- provide monitoring communications data requests and responses for the purposes of audit; and

CSPs will process requests from the automated system in order to enable coherent and consistent data to be disclosed to the requesting public authority.

6.1.3 Data acquired by Public Authorities

Once data has been disclosed by a CSP to a public authority (whether directly or through the automated system) the requesting authority becomes the Data Controller for that data. Where the automated system carries out processing (including temporary storage) this is done on behalf of the public authority as a Data Processor.

Note that a copy of disclosed communications data will continue to be stored by the CSP, and the CSP will remain the Data Controller for this data.

6.2 Subject Access Requests

The Data Protection Act gives the subjects of data the right to request access by making a Subject Access Request (SAR). An exemption to this exists for personal data that is being processed on the grounds of national security or for the “prevention or detection of crime” but only to the extent that complying with a particular request would prejudice the prevention and detection of crime. SARs are determined on a case by case basis and not subject to blanket exemptions.

A SAR made of a public authority would be exempt from disclosure if compliance would prejudice the prevention or detection of crime. This might for example occur if by disclosing that an authority held communications data on an individual that would indicate that an investigation is underway.

The code of practice under the proposed legislation will provide guidance on the relationship between disclosure of communications data under the Act and the provisions for subject access requests under the DPA, and the balance between CSPs obligations to comply with a notice to disclose data and individuals’ right of access under section 7 of the DPA to personal data held about them. As at present, there will be no provision preventing CSPs from informing individuals about whom they have been required by notice to disclose communications data in response to a SAR made under section 7 of the DPA. However a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA.

7. Relevant Legislation

1. OSA – Official Secrets Act 1911-1989.
2. EU DRD - European Union Data Retention Directive 2005 transposed in the UK’s Data Retention (EC Directive) Regulations 2009.
3. RIPA – Regulation of Investigatory Powers Act 2000.
4. DPA – Data Protection Act 1998.
5. FoIA – Freedom of Information Act 2000.
6. HRA – Human Rights Act 1998.
7. CMA – Computer Misuse Act 1990.
8. PACE – Police and Criminal Evidence Act 2003.
9. TCA – The Communications Act 2003.
10. CPIA – Criminal Procedures and Investigations Act 1996,
11. CPLA – Code of practice for legal admissibility 2008.

12. TR – Telecommunications Regulations 2000.

Annex A: Glossary

ATCSA - Anti-Terrorism, Crime and Security Act 2001

CCD – Communications Capabilities Development programme

CSP - communications service provider

DP - designated person

DPA - Data Protection Act 1998

DPP – Data Protection Principles

ECHR - European Convention on Human Rights

EU DRD - European Union Data Retention Directive

ICO - Information Commissioner's Office

IOCCO - Interception of Communications Commissioner's Office

ISP - Internet Service Provider

PECR - Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

PET – Privacy enhancing technologies

PIA - privacy impact assessment

RIPA - Regulation of Investigatory Powers Act 2000

SPoC - single point of contact

TAB - Technical Advisory Board

Annex B: Types of communications data

There are three types of communications data as defined in the Communications Data Bill.

- **Subscriber Data** – Subscriber data is information held or obtained by a provider in relation to persons to whom the service is provided by that provider. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it. Examples of subscriber information include:
 - subscribers or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
 - information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
 - information about the provision to a subscriber or account holder of forwarding/redirection services;
 - information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes.
 - information provided by a subscriber or account holder to a provider, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is not disclosed).
- **Use Data** – Use data is information about the use made by any person of a postal or telecommunications service. Examples of use data may include:
 - itemised telephone call records (numbers called);
 - itemised records of connections to internet services;
 - itemised timing and duration of service usage (calls and/or connections);
 - information about amounts of data downloaded and/or uploaded;
 - information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
 - information about the use of forwarding/redirection services;
 - information about selection of preferential numbers or discount calls;
- **Traffic Data** - Traffic data is data that is comprised in or attached to a communication for the purpose of transmitting the communication. Examples of traffic data may include:
 - information tracing the origin or destination of a communication that is in transmission;
 - information identifying the location of equipment when a communication is or has been made or received (such as the location of a mobile phone);
 - information identifying the sender and recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
 - routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer

logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);

- anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission;
- online tracking of communications (including postal items and parcels).

Annex C: Relevant legislation

The use of communications data in the investigation of crime is not new and pre-dated the Interception of Communications Act 1985 (now repealed). Legislation has been further developed since then to create more formal powers and safeguards.

7.1.1 IOCA - Interception of Communications Act 1985 (now repealed)

The Interception of Communications Act 1985 (“IOCA”) was passed partly to comply with the judgement in *Malone v UK (1984)*. IOCA placed the interception of communications sent by post or by means of a public telecommunication system on a statutory basis for the first time. Previously interception had not been openly governed by statute, but by codes of practice issued (but not made public) by the Home Office. The judgement in the *Malone* case found that this did “*not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred to the Public Authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking...*”

7.1.2 RIPA - Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) repealed the IOCA. The main purpose of the Act is to ensure that investigatory powers are used in accordance with human rights. Those powers include the acquisition of communications data and the interception of communications. .

RIPA (Part 1, Chapter 1) provides a legal framework governing Lawful Interception activities in the UK (interception being an operation to obtain the content of a communication and not just the associated data). Interception warrants must in general be issued and renewed by the Secretary of State personally, subject to strict tests of necessity, proportionality and legitimate aim. An interception warrant may only be issued on an application made by or on behalf of a small number of security, intelligence and law enforcement agencies. .

RIPA (Part 1, Chapter 2) deals with the specific topic of communications data. It sets out the powers, requirements and safeguards regarding data acquisition. Orders made under Chapter 2 specify the Public Authorities that are allowed to use RIPA to acquire communications data and limit the purposes for which they can do this and the types of communications data that they can acquire. RIPA requires a senior official, of a rank designated by parliament, to authorise each communications data request if, but only if, he believes the tests of necessity, proportionality of legitimate aim are satisfied.

There are two important further sources of safeguards in RIPA: a tribunal to investigate specific complaints, and a Commissioner to oversee the operation of the system of interception and the acquisition of communications data as a whole. The Commissioner’s oversight role helps to ensure that any given individual’s communications data is safeguarded in accordance with the legislation and that rigorous authorisation process is applied consistently by relevant Public Authorities. The Commissioner has a team of inspectors who work to ensure that Public Authorities fulfil the strict requirements of the law set out in RIPA and the statutory Code of Practice. Inspections of Public Authorities take place throughout the year and the Commissioner reports annually to the Prime Minister and his report is laid before Parliament. These inspections look at the proportion of the authorisations or notices or authorisation was of a sufficient rank and went through a full and thorough process of considering human rights.

RIPA provided for the creation of an independent Tribunal (‘the Investigatory Powers Tribunal’). The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data under the Act.

7.1.3 Anti-Terrorism, Crime and Security Act 2001

Part 11 of the Anti-Terrorism, Crime and Security Act 2001 (ATCSA) provides that the Secretary of State may issue a code of practice relating to the retention by communications providers of communications data obtained or held by them. The Code may contain any such provision as appears to be necessary: (a) for the purpose of safeguarding national security; or (b) for the purposes of prevent or detecting of crime or the prosecution of offenders (which may relate directly or indirectly to national security). The ATCSA allowed the Secretary of State to ask CSPs to retain, for a period of up to 12 months, data that they already held or obtained for their own business purposes. Its object was not therefore to enlarge the fields of data which a communications provider may (or must) retain, but to encourage providers to retain that data for longer than they would otherwise need to do so for their own commercial purposes

7.1.4 EU Data Retention Directive

The EU Data Retention Directive 2006 (Directive 2006/24/EC) requires every EU member state to require CSPs to retain certain types of communications data for at least 6 and up to 24 months.

7.1.5 Data Retention (EC Directive) Regulations 2009

The EU DRD was transposed into UK law by the Data Retention (EC Directive) Regulations 2009. The Regulations impose a requirement on public communications providers to retain the categories of communications data specified in regulations for a period of 12 months.



Annex D: Privacy enhancing technologies (PET) assessment

ICO Action	CCD Response
<p>Providing sample costs, risks and benefits cases to demonstrate the value of privacy compliance</p>	<p>The business case recognises privacy concerns and Communications Capability Development programme (CCD) is preparing a PIA.</p>
<p>Promoting a simple shared language for key privacy concepts such as data minimisation, identification, authentication and anonymisation to assist communication within and outside of organisations</p>	<p>CCD uses the concepts and language of data minimisation, identification and authentication. These concepts are used in communications with stakeholders. Most large CSPs will follow these principles as good business practice.</p>
<p>Incorporating Privacy Impact Assessments throughout the systems lifecycle from business case to decommissioning</p>	<p>PIAs are being prepared. Their whole system lifecycle applicability needs to be verified and ensured as systems are specified and procured.</p>
<p>Managing privacy-related risks to within pre-defined levels</p>	<p>Under review as part of continuing work on security architecture.</p>
<p>Potentially submitting Privacy Impact Assessments for the most sensitive systems to the ICO for verification</p>	<p>CCD is submitting the PIA.</p>
<p>Promoting greater transparency by publishing Privacy Impact Assessments</p>	<p>CCD will publish the PIA.</p>
<p>Demonstrate that all new systems support automated Subject Access Requests, and implement online Subject Access Request services where appropriate.</p>	<p>SARs for data held on CSP's systems are the responsibility of the CSPs. No CSPs offer online access. The decision to offer online access is a business decision for CSPs.</p>