# Communications Data Bill

## Introduction

Communications data is the information about a communication. 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. Communications data does not include the content of any communication – the text of an email or a conversation on a telephone. It is information about a communication – not the communication itself.

Communications data is used by the police and the security agencies in the investigation of all types of crime, including terrorism. It enables the police to build a picture of the activities, contacts and whereabouts of a person who is under investigation. It can be used as evidence in court. Communications data has played a role in 95 per cent of all serious organised crime investigations and every major Security Service counter-terrorism operation over the past decade.

New communications technologies are generating communications data in different ways. Not all this data is currently retained by communications/internet service providers, as they may have no business interest in doing so; the police and others are therefore unable to get access to it. This has a direct impact on the investigation of crime in this country and on our ability to prosecute criminals and terrorists. To ensure that communications data continues to be available to the police and others will require legislation.

This paper sets out key information about the draft Communications Data Bill published on 14 June 2012. The Bill itself and supporting materials are published separately and available through the Home Office website.

## 1. The current system

### What is communications data?

Communications data includes the time and duration of a communication, the number or email address which has been contacted and sometimes the location of the originator of the communication. It does not include the content of any communication – the text of an email or a conversation on a telephone. It is information about a communication – not the communication itself. The definitions and restrictions relating to communications data are clearly set out in the Regulation of Investigatory Powers Act 2000 (RIPA) which at present provides a legal framework for access to data by public authorities.

### Why is communications data important?

Communications data has played a role in 95 per cent of all serious organised crime investigations and every major Security Service counter-terrorism operation over the past decade. It is vital to law enforcement when dealing with organised crime gangs, paedophile rings and terrorist groups and is critical to everyday policing. It enables the police to build a picture of the activities and contacts of a person who is under investigation. Communications data is routinely used as evidence to support prosecutions in court.

### What happens now?

Companies providing communications services are required by law to store certain types of communications data where they have business reasons to generate or process it. The police and others can then apply to get access to communications data under RIPA if they can demonstrate that their request is necessary and proportionate. Access is on a case by case basis and is subject to independent oversight. The police have no power to get access to communications data where it is not connected to a specific investigation or operation.

The EU Data Retention Directive requires UK communications service providers (like those from all other EU states) to retain telephony and some internet-related communications data, which is generated or processed in connection with their business, for between 6 and 24 months. The retention period in the UK is 12 months. Critically the Data Retention Directive only requires the retention of data which companies collect for their own business purposes. And it does not apply to overseas providers.

**What different types of communications data are available?**

Definitions can be found within RIPA and a publicly available code of practice regarding the acquisition of communications data. In summary:

- **'Subscriber Information'** is information that private sector communications service providers (CSPs) hold about people to whom they provide a service (e.g. names, addresses, telephone numbers)
- **'Service Use Information'** is information about the use a person makes of a service (e.g. itemised telephone call records, records of connection to internet services, timing and duration of service usage)
- **'Traffic Data'** is information about a communication and the equipment used in transmitting it (e.g. information about the location of mobile phones, routing information such as IP address allocation)

**Do Communications Service Providers currently have to store any data?**

Some communications service providers already generate and process internet communications data for business use and retain it under a notice issued by the Government as a result of the EU Data Retention Directive. We do not comment on which communications service providers store data under a notice.

**Who has access to communications data?**

Only public authorities designated by Parliament can obtain communications data under RIPA for those purposes set out by Parliament. The list of authorities and purposes are set out in legislation. Law enforcement and security and intelligence agencies account for nearly 99% of requests for communications data. The police are the main user of communications data. They can obtain data where it is necessary to a specific investigation or operation.

Some other public bodies including some Government Departments, regulators and local authorities, have been granted access to some communications data under RIPA in order to discharge their investigatory or public protection responsibilities. Their requests account for around 1% of the total. The largest user of communications data outside of law enforcement and the intelligence agencies is the Financial Services Authority. Local authorities do not have access to all types of data and their data requests comprise less than 0.5% of the total. Other users of communications data account for a very small number of annual requests – over half of those in 2010 made fewer than 20 requests, the majority for basic subscriber data.

RIPA requires requests for data to be approved by senior officials or officers in the applying agency. Approval may only be given if an applicant is able to demonstrate that data is necessary in an investigation for a permitted purpose and proportionate to the objective of the investigation: an application must assess the benefits of the data which has been requested against intrusion into privacy. Local authorities will now need to get the approval of a magistrate under new provisions in the Protection of Freedoms Act 2012 (which are due to be brought into force in the autumn).

Details of the use of communications data are openly available in the annual report of the Interception of Communications Commissioner. A publicly available Code of Practice provides further detailed guidance on the above. Under any new legislation, Parliament would need to debate and approve which public authorities have access to communications data and for what purposes.

**Why can local authorities access communication data?**

Local authorities use communications data to investigate crimes such as trading standards offences, fly-tipping, and benefit and council tax fraud. These offences can have a significant impact on local communities. Local authorities do not have access to all types of communications data and in practice most of their requests are for subscribers to mobile telephones. Transferring these responsibilities to the police or other investigative or regulatory bodies would raise issues of resourcing, expertise and prioritisation of investigative effort for the body concerned. But this is an issue that pre-legislative scrutiny will no doubt want to consider.

**What are the current safeguards?**

There are well established safeguards within RIPA:

- Communications data may only be acquired under RIPA by public authorities that have been approved by Parliament to do so;
- Communications data 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);
- Data is obtained on a case by case basis and must be authorised by a senior officer at a rank stipulated by Parliament;
- The authorising officer may only authorise a request for communications data if the tests of necessity and proportionality are met in that particular case;
- 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 processing of personal information, including communications data, is regulated by the Data Protection Act 1998 which is overseen by the Information Commissioner;
- The Information Commissioner is under a duty to monitor the application of the provisions of the Data Retention (EC Directive) Regulations 2008 (which transpose into UK law the requirements of the EU Data Retention Directive) with respect to the security of stored data.

**How many Communications Data requests are there?**

Statistics collected by the Interception of Communications Commissioner show that in 2010 there were about 550,000 requests for communications data under the Regulation of Investigatory Powers Act (RIPA) 2000. Figures for 2011 will be released shortly.

Many requests for data may relate to the communications of a single person: data is ***not*** sought on 550,000 people.

The number of communications data requests reflects: the frequency with which communications services are now used, the levels of organised and serious crime, the ways in which criminals communicate and the value of communications data to policing.

In 2010 91% of the UK population owned a mobile phone and about 12 million had a smart phone. Smart phone usage continues to grow rapidly. In 2010 the call volume (fixed and mobile) was 254 billion minutes and there were 129 billion text messages sent – equivalent to five text messages per person per day.

Home Office published statistics show that there are in excess of 4 million crimes reported annually and around 1.4 million of these will fall into the serious crime category. Criminals will often use many communication devices at any one time and will regularly change them. A significant murder or organised crime investigation can involve up to 500 communications data requests or more – often mainly subscriber checks.

Communications data helps focus an investigation by identifying possible suspects, and is also critical in confirming alibis, ruling people out of further enquiries, and finding witnesses. Many tens of thousands of communications data requests are

made every year in urgent threat to life situations: e.g. to find a vulnerable or missing person or in kidnap situations.

The number of data requests therefore reflects the rapid growth in communications services and usage; the levels of serious and organised crime in this country (ie there are far more incidents of serious crime than there are requests for data); and criminal use of communications devices.

**How does the UK compare to other EU countries in its usage of CD?**

Nearly half of EU Member States have not to date provided statistical returns on their use of communications data. There are also differences in the way in which Member States have interpreted the obligations to make statistical returns leading to inconsistencies in these returns.

Of the 15 Member States who provided data in the last year of available statistics (2009), the UK was the third largest requestor of DRD data (making 363,104 requests) after France (514,813) and Poland (1,048,318). Twelve Member States provided no figures.

EU DRD statistics are calculated on a different basis to that used by the UK domestically – hence the difference between the UK's domestic and EU published statistics.

**Many EU partners have judicial authorisation – why can't we?**

There are different systems across Europe reflecting different criminal justice systems. What is important is accountability and that those authorising the requests can ensure that proper consideration is given to necessity and proportionality. The UK has a common law system in which the police direct criminal investigations and bring charges. In many continental systems, prosecutors and the judiciary are more directly involved in directing investigations and bringing charges. In many of these countries communications data requests are authorised by prosecutors or investigating magistrates.

In the UK, authorisation of communications data requests is provided by a senior officer unconnected to the investigation concerned, and is based on a detailed application by the investigating officer and advice from a trained expert in communications data (the Single Point of Contact). The senior officer may only approve a request if they are satisfied that the tests of necessity and proportionality are met. Use of the powers is subject to regular inspection by the Interception of Communications Commissioner who sets out his findings annually in a published

report. The use of communications data in support of prosecutions in court is subject to challenge and scrutiny in the courts in the normal way.

There would also be practical and operational constraints in requiring prior magistrate approval. Local authority requests for communications data constitute less than 0.5% of total requests each year. It is logistically possible to submit these requests to a magistrate. Under existing resources it is not possible to do the same for the much greater number of requests from policing which are also often much more urgent and operationally sensitive. There would need to be a major increase in the number of magistrates available across the country, including some 24/7, to approve communications data requests. Some Magistrates may need to receive security vetting.

In the UK the reporting requirements and oversight provided by the Interception Commissioner ensures that we know, for example, how many communications data requests are made. Others in Europe, who have judicial authorisation, can struggle to get this information because there is no mechanism for recording the number of requests.

Introducing prior judicial authorisation for communications data requests in the UK would be expensive, logistically challenging, affect police and intelligence agency investigations and be a significant change to our criminal justice system and the relationship between police, intelligence agencies and the judiciary.

**How is communications data used in prosecutions?**

In a criminal trial, the prosecution case will involve a variety of different types of evidence, including communications data. For example, the CPS Organised Crime Division brought ten cases to trial during April 2012 and relied on communications data in eight, including six cases of drug trafficking or conspiracies to supply controlled drugs, and two money laundering cases. The remaining two prosecution cases were financial crime cases brought as the result of a reactive investigation. In one case, communications data was used in the initial investigation, and in the other case in communications data was used in evidence in an earlier trial related to the case.

A separate study was conducted by the Metropolitan Police Service (MPS) between April 2009 and March 2010 looking at various aspects of how prosecutions were supported. This showed that during this period traffic data was used in 200 prosecutions (primarily murder, armed robbery, kidnap and trafficking offences). Court results indicate 82% of the defendants were found guilty, 14% pleaded guilty, and 4% were acquitted. It is not possible to quantify exactly how communications data directly contributed to these results, but those involved in bringing these

prosecutions observed that the extent to which communications data is used to corroborate other evidence, including witness statements, evidence of location, association and chronology should not be underestimated.

**For which purposes do the police request communications data?**

In 2010 we carried out a 2-week nationwide survey of police communications data requests for all crime except terrorism (The Met Counter Terrorism Command were unable to participate in this survey due to operational pressures). The findings were as follows:

- 11.4% of requests for communications data related to murder investigations
- 2.7% for kidnap, extortion and blackmail
- 12.3% for sexual offences
- 26.1% for drugs trafficking
- 0.9% for people trafficking
- 29.3% for other serious crime
- 17.3% for other non-serious crime

'Other serious crime' will include a range of offences including violence against the person, robbery, fraud, forgery and firearms offences.

It is important to state that the data from these surveys represents a snapshot from a limited period of time – the statistics may be affected disproportionately by particular investigations in progress at the time of the survey and should therefore be treated as indicative rather than definitive. We are conducting a new survey to see whether this has changed but the results are not yet available.

## 2. The need for new legislation

**What is the problem?**

New communications technologies are generating communications data in different ways. Not all this data is currently generated, collected or retained by communications/internet service providers, as they may have no business interest in doing so; the police and others are therefore unable to get access to it and it cannot otherwise be retrieved for the purpose of facilitating a criminal investigation. This has a direct impact on the investigation of crime in this country and on our ability to prosecute criminals and terrorists.

To ensure that communications data continues to be available to the police and others will require legislation. We cannot rely on existing data retention legislation alone because that only requires companies to retain data which they collect for their own business reasons and because it does not apply to providers based outside the UK but who offer services to UK users (eg webmail). As technology and business models have changed, less of the information that the police and others require is being retained

**What do we plan to do about it?**

The Government is introducing legislation to ensure communications data will continue to be available in the future as it has been in the past and that the police and agencies can continue to get access to it. The data will be available only when a request is authorised by a designated senior officer, on a case by case basis, in accordance with the law and the process will be overseen by the Interception of Communications Commissioner, as it is now. Communications technology will continue to rapidly evolve. Our proposed response is therefore intended to be flexible and avoid solutions that may be superseded even before they are complete. It is technically feasible.

**What would be the impact if nothing is done?**

If new legislation was not introduced law enforcement and other designated bodies will increasingly be unable to access the communications data they need to develop their investigation. This would have a direct and tangible impact on public safety as criminals would find it increasingly possible to operate without fear of being detected.

**What evidence do you have that the absence of data is causing operational difficulties for the police and others?**

At present, approximately 25% of communications data required by the police and agencies can no longer be acquired because the relevant data is not available at the necessary quality and timeliness to support operational needs. The situation will degrade further unless action is taken. If the proposals in the draft Bill are passed into law, we assess that we will be able to halt and reverse much of the recent significant degradation

The Child Exploitation and Online Protection agency (CEOP) is responsible for the investigation of child exploitation in the UK. CEOP is already experiencing significant problems because of the difficulty of obtaining the same level of subscriber information for internet communications as is currently available for traditional telephony. These problems are being encountered across all areas of policing. Sufficient, reliable communications data is no longer always available when needed, or in a usable form, or for the range of services required.

**Won't these proposals simply force criminals to use services which are harder to investigate?**

Criminals and terrorists will always seek to hide their activities and hinder investigations by law enforcement authorities, including by using services or adopting behaviours which they believe make them harder to detect. The proposed legislation will provide the flexibility to help maintain investigative capabilities in the face of changes in technology and criminal behaviour. Our approach will be intelligence-led – if we assess that criminals are using particular services or techniques to try to hide their activities, we will adapt our approach to counter them.

As is well-established practice, we cannot comment publicly on the methods or technologies we might use to respond to changes in criminal behaviour.

## 3. What will the legislation do?

**What will the legislation do?**

We need to make sure that, when we judge it to be necessary, communications service providers – including CSPs, telephone and mobile companies – keep information on how customers use their services. The Bill will:

- Enable the Home Secretary, when necessary, to require Communications Service Providers to retain data where they would not otherwise retain it for business reasons.
- Enable this data to be provided to public authorities efficiently and with the minimum possible impact on individuals' privacy.
- Extend safeguards
- Replace existing communications data access provisions in RIPA, which will henceforth cease to deal with communication data.

**What obligations will you be placing on CSPs?**

We will not place new obligations on every CSP, or in relation to all communication services. New obligations will be subject to detailed discussion with legal, commercial and technical representatives from CSPs and only then will a decision be taken on the detailed obligations that should be placed on the CSP.

These will be agreed by the Secretary of State who will set out the detailed obligations to be placed on any provider in a notice. The notices will describe, on a service-by-service basis, the description of data which must be retained, where the data should be stored and, if necessary, how the data should be collected.

**Are you going to ask overseas operators to retain/generate data?**

In principle this legislation will cover overseas operators where they provide communications services in this country. We will therefore be working with providers in the UK and overseas as we do already. For security and commercial reasons we do not comment on relationships with specific providers.

**How long will data have to be retained by CSPs?**

CSPs will be required to retain the communications data they hold under obligations in the Bill for up to a maximum of 12 months. This is consistent with the UK's

implementation of the European Data Retention Directive. After the end of the 12 month period, CSPs will be required to destroy data retained under these obligations in such a way that it can never be retrieved.

**Why don't you ask CSPs to retain the data of only people under criminal investigation?**

It is impossible to know in advance of a crime or a criminal investigation whose data will need to be investigated and whether those people are suspects or victims.

In order for the police and others to be able to access data when they need it, for example to investigate a murder or locate a person at risk, the data has to have already been retained. If it has not been retained, it cannot otherwise be retrieved at the moment it is needed and access to it is not therefore possible.

The data that has been retained by CSPs will only be accessed by authorised public authorities on a case by case basis and where this relates to a specific operation or investigation.

**Will the new legislation require CSPs to collect and hold new data which they do not already collect and hold for their business purposes?**

In some cases, yes. New business models mean some of the communications data now needed by the police and others is not always required and retained by service providers for business purposes. New legislation will allow us to work with the communication service providers to ensure this data is available, so that on a case by case basis the police and others may then seek access to it.

**Will CSPs be required to record website visits?**

Under existing legislation and practice, the definition of communications data already includes data about websites which have been accessed. It also includes data about communications accessed through a website. But it does not and will not include the content of specific pages that have been browsed within a website. Communications data detailing which websites customers visited (but not the specific pages) has been capable of being retained by communications service providers since 2001, where they have agreed to cooperate under a Voluntary Code of Practice on retention of communications data.

**Will this cover social media, messaging services etc?**

Public websites, including public Facebook pages, are open to all to browse and are not affected by this legislation; this legislation only covers access to communications data, including for example, data regarding e-mails and instant messaging. This legislation can apply to all providers of telecommunications services. For security and commercial reasons we cannot comment on obligations which have been or may be placed on specific providers.

**How is this proposal consistent with coalition commitments to end the storage of communications data without good reason?**

At present, for business reasons, communications providers store some of the data to which we may need access. In future, under this legislation, we will only ask communications providers to store any additional data (beyond that provided for at present) if there is reason to believe that the services from which it derives are being used by terrorists, people engaged in serious crime or other people under investigation by the police or other authorised agencies. A maximum time limit of 12 months will be placed on storage, consistent with the terms of the EU Data Retention Directive. In short: there will have to be good reason for Government to require both the collection and storage of communications data.

The Government set out its intention to legislate on this issue in the Strategic Defence and Security Review (SDSR) which was published in 2010. The SDSR made clear that we would legislate as soon as parliamentary time allowed, ensuring that the use of communications data is compatible with the Government's approach to civil liberties.

**Isn't this a resurrection of the Interception Modernisation Programme (IMP) from the last Government**

There are significant differences between this programme and the programme developed by the last Government.

We are not proposing a single Government database to store all communications data to which the police would then have access.

The IMP included plans for the widespread deployment across UK communications networks of technical probe equipment (sometimes loosely described as 'black boxes') to collect communications data generated from communications services. This would have involved the collection of communications data about certain types of services by UK network providers – who may have provided the connection to the

internet, but not the specific service itself. Under this programme, the emphasis is to work with industry to determine the best solution on a case by case basis, examining services used by people under investigation by the police or other authorised agencies. Probes would only be used when this approach did not provide the communications data required. Any communications data collected by such probes would, as with other data, be stored by the industry.

**How can you distinguish between communications data and communications content**

We are confident that the technology we and CSPs would be using can distinguish between communications data and content. We are not proposing to legislate to obtain communications content.

Any attempt to create a system that bypasses the existing legal framework for interception would be unlawful.

The Bill states explicitly that nothing in the provisions in Part 1 "authorises any conduct consisting in the interception of communications".

**How much will implementing these proposals cost?**

The estimated economic cost of the programme in the period from FY2011/12 until 2015/16 is up to £800 million. (This is the amount the programme would cost less inflation, irrecoverable VAT and depreciation.)

It is difficult to estimate costs over the longer term: the programme has an incremental approach to developing capabilities, which responds to changes in technology and the communications market place. These changes are difficult to predict. Costs will be kept constantly under review and the business case will be refreshed on a regular basis.

Our current estimates are that the economic costs of this programme over ten years from 2011 could be up to £1.8 billion.

These costs need to be set against total policing costs and against anticipated financial benefits.

An investment of about £180m a year in communications data amounts to just 1.3% of the current annual £14 billion policing budget.

But communications data plays a key role in the investigation and prosecution of all types of crime. Over ten years, we assess that this work will give measurable

benefits of approximately £5–6 billion. This includes conservative estimates of direct financial benefits (assets seized, revenue lost etc). There are also benefits to which it is difficult to ascribe a financial value, for example seizures of drugs, disruption and prosecution of terrorists and improvements in operational efficiency.

**Are there cheaper alternatives?**

No. The use of communications data is often the most efficient option for securing evidence. It supports many criminal investigations and rapidly and reliably enables the police to better understand the activities and contacts of a suspect.

Alternative methods of investigation, such as directed surveillance or undercover officers, cost significantly more than communications data, do not provide the same level of benefit and in some cases would be more intrusive. Alternative methods such as surveillance cannot provide essential historical information required in criminal investigations.

**Who will bear the cost?**

The communications industry is already reimbursed by Government for costs incurred in the provision of communications data. This arrangement will continue under the proposed legislation.

## 4. Safeguards

**What safeguards will there be?**

There will be safeguards at every stage of the communications data process, including access, data retention, oversight and appeals (both by CSPs and individuals).

Only four bodies – the police, Serious and Organised Crime Agency/National Crime Agency, Her Majesty's Customs and Revenue and the intelligence agencies – will be granted access to communications data through this bill. Other public bodies who currently have access to communications data will only continue to do so following debate and approval by Parliament and if that access is considered vital to protecting the public or investigating crime.

Access to communications data will only be able to be obtained for a specific purpose (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) and by those public authorities authorised to do so. Requests for data will need to be approved by senior designated officers in the applying agency. Necessity and proportionality will be the key criteria that must be met in each case.

Following the Protection of Freedoms Act 2012, local authorities will be required to secure judicial approval before obtaining communications data (or using any Part 2 RIPA technique). The local authority provisions in the Protection of Freedoms Act will come into force in the autumn.

Filtering arrangements will be put in place to ensure that only the data relevant to a request will be passed on to the public authority seeking the information and that any data not directly relevant will not be disclosed.

The Interception of Communications Commissioner will provide independent oversight of the acquisition of communications data by public authorities. The role of the Commissioner will also be extended to oversee the new powers, including the collection of communications data by communications service providers. This will include oversight of testing, regular auditing and inspections.

The communications industry will be required to ensure that data retained under this legislation is protected against accidental or unlawful destruction, accidental loss and unauthorised access or disclosure. Legislation will make explicit that all communications data retained by CSPs under the legislation will be destroyed after the 12 month retention period (unless required for legal proceedings).

The legislation will provide for the Information Commissioner to keep under review the security and integrity of the communications data retained e.g. against accidental loss, unlawful destruction, unlawful retention and unauthorised disclosure, consistent with the Data Protection Act. There is also provision for the Information Commissioner to keep under review the specific requirement to destroy data when its retention is no longer lawfully authorised (e.g. at the end of a retention period specified under the new provisions).

If a communications service provider is concerned about the requirements placed upon them, it can ask an independent Government / Industry body (The Technical Advisory Board) to consider the impact of these obligations. The Technical Advisory Board would then advise the Secretary of State on whether the obligations should be maintained, modified or removed.

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.

**What are the penalties for misusing or failing to appropriately secure communications data which has been retained by CSPs?**

Processing of communications data must comply with the requirements of the Data Protection Act (DPA) 1998 and serious breaches of the DPA can incur fines of up to £500,000. The DPA gives the Information Commissioner's Office (ICO) powers which help to protect personal information 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.

- All of these safeguards apply to communications data (that is personal data as defined by the DPA) retained by CSPs or acquired by public authorities.

**What are the penalties for public officials or others abusing access to personal data?**

A number of offences exist on the statute books and in the common law to address situations where public officials, and other individuals, abuse access to personal data. In many cases, the obtaining of personal information is likely to be part of a course of conduct involving criminal activity such as misuse of computer systems and hacking, all of which are offences. The relevant offences, depending on the context, may include:

- Unauthorised access to computer material, contrary to Section 1 Computer Misuse Act 1990 which carries a maximum sentence of two years' imprisonment;
- Unauthorised access with intent to commit another offence, such as fraud, contrary to section 2 Computer Misuse Act 1990 which carries a maximum sentence of five years' imprisonment;
- Knowingly or recklessly obtaining, disclosing or procuring the disclosure of personal data without the consent of the data controller under Section 55 of the Data Protection Act, which carries a maximum penalty of an unlimited fine;
- The common law offence of misconduct in public office. It is committed when the office holder acts (or fails to act) in a way that constitutes a breach of the duties of that office. The maximum penalty for this offence is life imprisonment.

In addition to the offences listed above, there are also a number of offences which may be relevant depending on the context, including offences of bribing another or being bribed contrary to the section 1 or 2 of the Bribery Act 2010. Where the offences were committed prior to the coming into force of the Bribery Act 2010, relevant offences include corruptly accepting money or other advantage contrary to section 1 of the Prevention of Corruption Act 1906 for which the maximum penalty is seven years' imprisonment.

**What are the penalties for unlawful interception?**

RIPA sets out the penalties for both intentional and unintentional unlawful interception.

A person convicted of intentional unlawful interception faces a criminal sanction of up to two years imprisonment, a fine (currently up to £5,000 on summary conviction), or both. If convicted in the Crown Court, there is no upper limit to a fine.

A person convicted of unintentional unlawful interception, is subject to a civil sanction which allows fines of up to £50,000 to be imposed. The independent Interception of Communications Commissioners is responsible for investigating cases of unintentional unlawful interception and administering any sanctions.

## 5. Myths about the proposals

**The legislation will *not...***

- provide the police and others with new powers or capabilities to intercept and read emails and phone calls.
- provide the police and others with unregulated access to all forms of communications data.
- create a single Government database containing the records or the content of emails and phone calls..
- require every provider of every communication service in this country to collect every item of data generated by their services.
- allow Local Authorities greater powers.
- create new powers for the intelligence and security agencies.

## 6. Structure of the Bill

### Part 1: Ensuring or facilitating the availability of Communications Data

Part 1 of the Bill builds on existing communications data legislation and will sit alongside the Data Retention (EC Directive) Regulations 2009. Telecommunications operators are currently required by law to keep some communications data if they generate or process it for their own business reasons. Industry innovation means that companies no longer have the same data as in the past. Part 1 of the Bill provides new powers for the Secretary of State to require a company to obtain communications data that it would not otherwise have a business need for, to ensure that data is available to be obtained by public authorities. Part 1 also imposes safeguards in relation to data held by companies, including (for example) the security and integrity of that data.

### Communications Data duties notified to companies

An order made by the Secretary of State under clause 1 will set out the general nature of the requirements on companies to ensure or facilitate the availability of data. The range of potential requirements takes into account the constant evolution of services by operators. Part 1 sets out the parties who must be consulted before an Order is drafted. The requirements imposed could include those to generate or collect communications data the company does not have, to process communications data in specified ways and to keep the data safely and securely for up to 12 months.

The Secretary of State will impose more specific requirements or restrictions on each company by notice. The emphasis will be to ensure communications data can continue to be obtained from the operators of particular communication services, but only when there is a reason to believe these services are being used by people under investigation by the police or other public authorities. It will be necessary for certain companies to collect communications data for some overseas services. The Secretary of State will also require that the reliability of communications data is verified and that the data is promptly available.

A company will be able to refer a notice to the Government/industry Technical Advisory Board. The Secretary of State will consider the Board's conclusions and may withdraw, amend or confirm the duties which are to be imposed.

Part 1 of the Bill enables the Secretary of State to take civil proceedings against a company if it fails to comply with a requirement placed upon it.

**Security of the data and other safeguards**

Part 1 makes express provision for safeguards in relation to data held by companies. These safeguards include requirements relating to data security and integrity, retention periods, access to the data and destruction of the data at the end of the retention period. The Information Commissioner will keep under review the security and destruction of communications data. The role of the Interception Commissioner will be extended to oversee companies' performance of other Part 1 duties.

## Part 2: Regulatory regime for obtaining data

Part 2 of the Bill preserves the essential elements of the existing statutory framework which is used to obtain communications data from companies (Part 1 Chapter 2 of the Regulation of Investigatory Powers Act 2000).

The substantive protections of Article 8 (right to respect for private and family life) of the European Convention of Human Rights will continue to be guaranteed by the new statutory framework. In particular, an authorisation to obtain communications data may only be granted if the tests of necessity and proportionality are satisfied and it is necessary to obtain the communications data for a permitted purpose. In addition, Part 2 provides that it must be necessary to obtain the data for the purposes of a specific investigation or operation.

The existing regime of acquiring communications data by either authorisations (to obtain communications data) or notices (to a telecommunications operator to disclose communications data) is rationalised, providing a clearer basis for authorising the conduct necessary to obtain the data.

### Filtering of communications data and protecting privacy

Technical aspects of some communication services can make it harder to obtain the communications data about a single communications event. Data about a single event can be distributed across a number of communications service providers who collaborate together to deliver a service. Moreover, subscribers very often have no need to register with a service in their own names: anonymous communications are common. The effect of these issues is that greater analysis of communications data can be required to identify the key facts about a communication.

Part 2 of the Bill addresses these problems by providing a power to establish filtering arrangements.

These filtering arrangements will initially assist a public authority (mainly the police) to determine what data might be needed to identify key facts about a communication and to enable the authority to consider if the request for such data remains necessary and proportionate. If the request is then authorised, the filtering arrangements will obtain communications data from companies, process and then filter it to the point where the key facts about a communication have been established. At that point these key facts will be disclosed to the public authority making the request and all other data will be immediately destroyed. An audit log will be generated for inspection by oversight authorities.

The filtering arrangements will protect privacy by minimising necessary interference with the rights of telecommunications users. Less information will be provided to the public authority than would be the case if the filter was not available.

The Bill makes the Secretary of State responsible for setting up and maintaining any filtering arrangements and provides the power to transfer this to a designated public authority. Legal responsibility for ensuring the effective and lawful operation of any filtering arrangements will remain with the Secretary of State or other designated public authority to whom that responsibility is transferred. Operation of the filtering arrangements will be carried out by an approved body and overseen by the Interception of Communications Commissioner.

### Safeguards and oversight

The remit of the Interception Commissioner will be extended to oversee the filtering arrangements. Part 2 contains significant safeguards relating to the proper testing and functioning of the filter, security against unauthorised access, rigorous oversight and control and reporting to the Commissioner.

## Part 3: Scrutiny and Other Provisions

Part 3 of the Bill ensures that there is independent oversight of functions relating to communications data under Parts 1 and 2 of the Bill, as well as other supplementary provisions.

### Oversight by the Interception of Communications Commissioner

The Interception of Communications Commissioner will continue to provide independent oversight of the obtaining of communications data by public authorities under Part 2 of the Bill. Part 3 of this Bill also extends the role of the Interception of Communications Commissioner to oversee Part 1 of the Bill, including the obtaining of communications data by communications service providers. This will include oversight of testing, regular auditing and inspections.

### Oversight by the Information Commissioner

Part 3 of the Bill will provide for the Information Commissioner to keep under review the operation of any provisions relating to the security of communications data retained by communications service providers e.g. against accidental loss, unlawful destruction, unlawful retention and unauthorised disclosure, consistent with the Data Protection Act. There is also provision for the Information Commissioner to keep under review the specific requirement to destroy data when its retention is no longer lawfully authorised (e.g. at the end of the maximum 12 month retention period specified under the new provisions).

**Investigatory Powers Tribunal**

The Investigatory Powers Tribunal was established under the Regulation of Investigatory Powers Act 2000, to provide an appropriate forum for complaints or proceedings relating to conduct by public authorities under that Act. The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of Government. It has full powers to investigate and decide any case within its jurisdiction, which includes conduct relating to the obtaining of communications data. Part 3 of this Bill makes sure that the jurisdiction of the Investigatory Powers Tribunal is extended to cover conduct under Parts 1 and 2 of the Bill.

**Removal of other statutory powers with weaker safeguards which are currently used by public authorities to acquire communications data**

Information-gathering powers currently exist in other legislation which could be used by public authorities to acquire communications data. For example, the Social Security Administration Act 1994 (as amended by the Social Security Fraud Act 2001) is used by both the Department for Work and Pensions and local authorities to acquire communications data to investigate benefit fraud.

Part 3 of the Communications Data Bill will amend certain powers in other legislation so that they may not be used in the future to oblige communication service providers to disclose communications data. This is intended to ensure that the acquisition of communications data is subject to the safeguards in this Bill that ensure necessity and proportionality is considered in each case, independent oversight from the Interception of Communications Commissioner, and the ability for individuals to complain to the Investigatory Powers Tribunal if they feel their data has been acquired improperly.

**Contribution towards operators' costs of compliance**

Part 3 of the Bill will enable the Government to contribute towards the costs incurred by communications service providers or postal operators in complying with the new obligations (as for existing obligations under the Regulation of Investigatory Powers Act 2000). A contribution may be made to costs incurred, or likely to be incurred, as a result of the activities permitted or required by Parts 1 and 2 of the Bill. Certain conditions can also be placed on these contributions, for example a requirement to comply with any audit that that may reasonably be required to monitor the claim for costs. Whether contributions should be made and the appropriate level of contribution will be determined by the Secretary of State. At present, the Government meets operators' costs of complying with obligations in full.