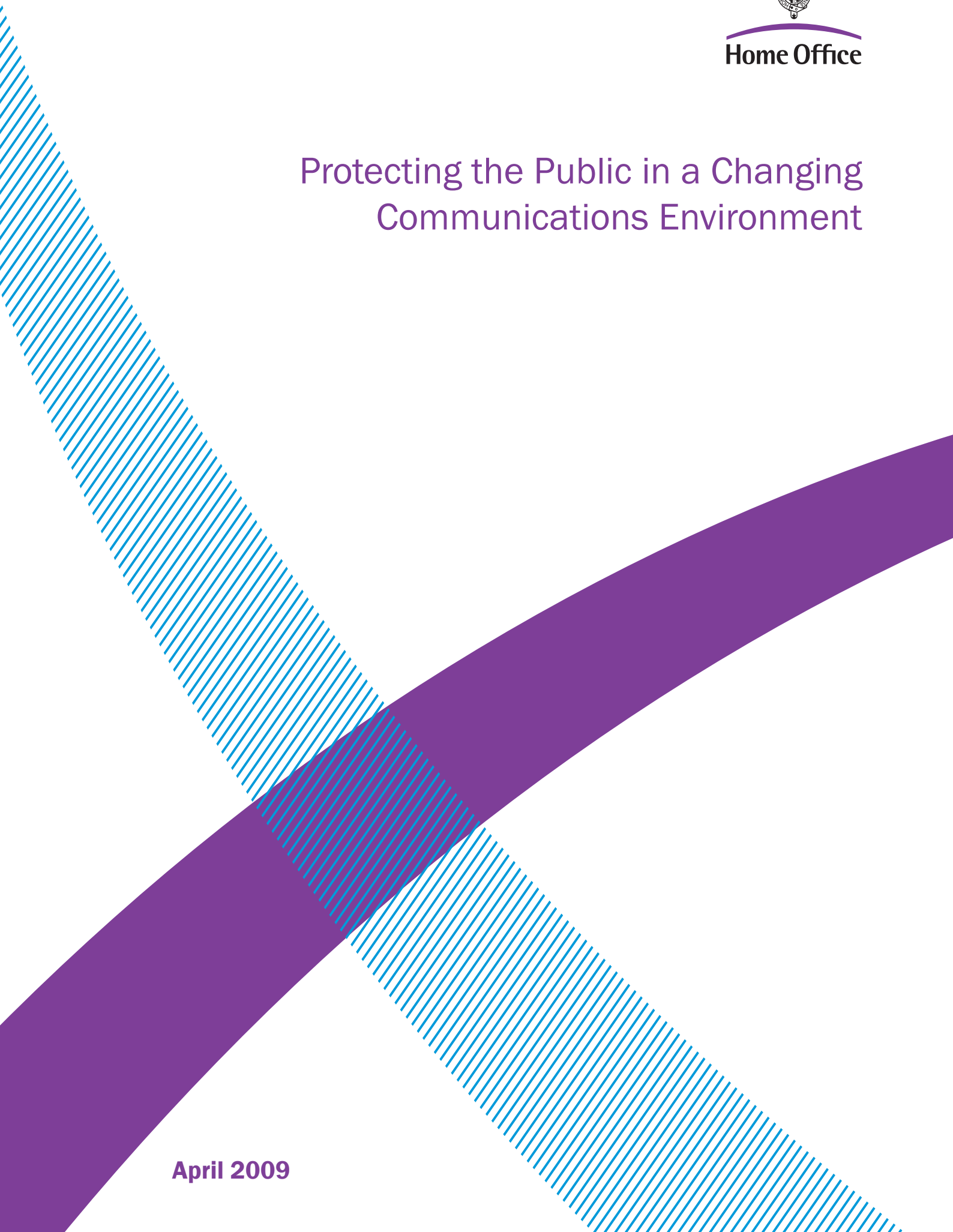
Home Office

Protecting the Public in a Changing Communications Environment



April 2009

Protecting the Public in a changing Communications Environment

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

April 2009

Cm 7586

£14.35

ISBN: 9780101758628

Contents

FOREWORD

By the Rt Hon Jacqui Smith MP, Home Secretary

We set high standards for our police, security and emergency services in keeping us safe and bringing criminals to justice. But we also expect our right to privacy to be protected too. That balance is at the heart of this consultation.

Used in the right way, and subject to important safeguards to protect individuals' right to privacy, communications data can play a critical role in keeping all of us safe.

For the police, the security and intelligence agencies, and other public authorities like the emergency services, being able to use the details about a communication – not its content, but when, how and to whom it was made – can make all the difference in their work to protect the public.

Governed by a strict regulatory framework, communications data is routinely used to investigate terrorist plots, to bring to justice those guilty of serious crimes, to seize illegal drugs and to protect the vulnerable in our society. It is no exaggeration to say that information gathered in this way can mean the difference between life and death.

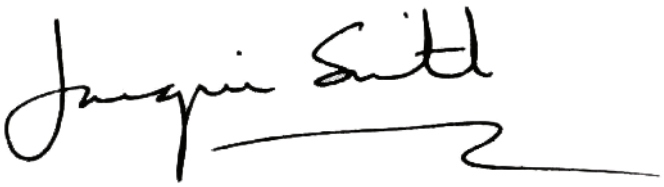
However, rapid technological changes in the communications industry could have a profound effect on the use of communications data for these and other purposes. The capability and protection we have come to expect could be undermined. This consultation sets out these changes in some detail, and the Government's proposed response to them.

I am clear that to do nothing in the face of these developments – thus allowing the capability to use communications data to degrade – could lead to more crimes left unsolved and more cases where public authorities could not protect people from harm.

I also know that the balance between privacy and security is a delicate one, which is why this consultation explicitly rules out the option of setting up a single store of information for use in relation to communications data.

My intention is to find a model which avoids the dangers of these two extreme positions, and which strikes the right balance between maximising public protection and minimising intrusion into individuals' private lives.

I look forward to hearing your views.



Jacqui Smith MP

SUMMARY

1. This consultation concerns the collection and use of 'Communications Data' (CD), an important technical capability that is used today to protect the public. This existing capability is declining in the face of the rapidly changing communications industry and we need to make changes if it is to be maintained in future. This paper outlines ways to do so.

2. Communications data is information about a communication. For a telephone call it can include the number called, from where and when, and who is the registered owner of that number. Communications data does not include the content of a call or the content of any other communications event, such as an email. This consultation does not propose changing the law to collect or store the content of any communication.

3. The communications service providers (anyone who offers a public telecommunications service such as a fixed or mobile telephone system, an email service, a broadband service or an internet service) currently retain communications data for their own business purposes. They typically store this data themselves and use it for billing, marketing, customer service, maintaining their networks and for quality of service monitoring.

4. Some public authorities, specified by law, can acquire communications data on a case-by-case basis from the communications service providers to enable them to carry out their duties to protect the public. These public authorities include the Police, the Serious Organised Crime Agency, Her Majesty's Revenue and Customs and the intelligence agencies; although other Public Authorities do have access to communications data limits have been placed on the type of data to which they can have access.

5. The ability to lawfully access communications data held by communications service providers is a vital tool for fighting and solving crime. It enables investigators to identify and build a picture of a suspect; provides vital clues in solving life-threatening situations such as kidnapping; creates evidence for alibis and prosecutions; supports lawful interception; and it helps the emergency services to help or locate vulnerable people. It is also critical to safeguarding the UK's national security, and in particular to countering the terrorist threat.

6. Communications data is used extensively as evidence in court, notably prosecutions for serious crime and terrorism. It has proved essential in convicting the guilty.

7. The ability of public authorities to access specified communications data is protected by safeguards under a detailed regulatory and legal framework. This ensures that any interference with the right to privacy through the acquisition of communications data is necessary and proportionate in any given case.

8. The majority of communications data held by communications service providers is never acquired by the authorities, since there is no justifiable need or reason to do so; there is no intention to change this under any of the options set out in this consultation paper.

The Safeguards

9. At the heart of Government policy in this area has been the imperative to strike a careful balance between the need for potentially intrusive investigative techniques and the right to privacy. Establishing an appropriate balance in this respect is also an important part of the Government's wider national security and counter terrorism strategies. The regulatory framework set up by the Government, and described in this document, is based upon the principles of necessity, proportionality, oversight and accountability. In particular, although large amounts of data are necessarily retained by the communications service providers both for their own business and national security reasons, access by public authorities to any of that data is tightly controlled.

10. Whatever approach the Government adopts, it will be critical to ensure that the regulatory and oversight arrangements remain effective. The more active or potentially intrusive the approach, the greater the need to modernise the safeguards to ensure that data is protected from abuse.

The challenges

11. The communications industry is highly competitive and technologically driven. The UK is currently undergoing the most significant communications changes since the development of the telephone as a competitive market encourages companies to find new ways to offer more services and cut costs. BT, the largest network provider in the UK, is currently in the process of rolling out a nationwide network based on Internet Protocol.

12. As a result of these technical changes, companies will offer more communications services, for voice, data and media, and including TV, social networking, music, video messaging, games, text, email and internet browsing. Some new services will be offered by the companies that operate the existing communications networks. Others will be offered by companies, some based overseas, providing services without any physical networks of their own.

13. These changes will have a significant impact on the ability of public authorities to continue to access, and use, communications data as they have done in the past. The proportion of communications data that is retained by communications service providers in the UK, and therefore accessible to the authorities, will decline. That data will be more fragmented if it crosses the networks of several communications service providers.

Options and solutions

14. The Government believes it must take action to maintain the existing capability which is available to some public authorities. Doing nothing is not an option: crimes that are currently detected would not be detected in the future; lives that are currently saved may be lost.

15. The Government therefore established the cross-government Interception Modernisation Programme (led by the Home Office) to examine how to maintain our communications data capability in the light of the challenges arising from the rapidly changing communications environment.

16. The Government has no plans for a centralised database for storing all communications data. An approach of this kind would require communications service providers to collect all the data required by the public authorities, and not only the data required for their business needs. All of this communications data would then be passed to, retained in, and retrieved from, a single data store. This could be the most effective technical solution to the challenges we face and would go furthest towards maintaining the current capability; but the Government recognises the privacy implications of a single store of communications data and does not, therefore, intend to pursue this approach.

17. There are two alternative ways to address the challenges which both aim to strike the right balance between privacy and security. They would require legislation to ensure that the data required by public authorities to protect the public is collected and retained by the communications service providers. This would include both the data that UK communications service providers already collect for their own business purposes and some additional data, largely relating to communications services provided from overseas providers, referred to in this document as third party data.

18. The responsibility for collecting and retaining this additional third party data would fall on those communications providers, such as the fixed line, mobile and WiFi operators, who own the network infrastructure.

19. This approach would ensure that all the relevant data was available to investigators but it would not address the problem of fragmentation. If communications data is distributed around a large number of separate data stores belonging to different communication companies, it would be harder and much slower for investigating authorities to piece it together. A further step would be for the communications service providers to process the third party communications data and match it with their own business data where it has elements in common; this would make easier the interpretation of that data if and when it were to be accessed by public authorities.

20. The Government recognises that any option focused on communications companies would put additional demands on industry, especially around the collection and retention of third party communications data not normally required for their own business purposes. The Government is therefore actively seeking the views of industry on these proposals through this consultation to help us meet Better Regulation commitments to minimise the costs and impact on the private sector.

Conclusion

21. This consultation covers an important topic that affects us all. The capability to use communications data to protect the public is being eroded by new technology. In seeking to maintain that capability, the Government must strike the right balance between public safety and privacy.

22. This document poses a number of questions to which the reader is encouraged to respond.

INTRODUCTION

This document sets out what communications data is and the vital role it currently plays in helping our law enforcement, security and intelligence agencies and emergency services to protect the public.

It explains how rapid technological changes in the communications industry threaten the ability of public authorities to use communications data to do in the future what they can do now. It sets out a range of options for what the Government might do to prevent this loss of capability. It also examines the privacy implications of this work, and describes current and possible future safeguards against unnecessary intrusion into people's lives.

The document asks various questions, on which the Government would welcome your views. These questions are summarised at Annex A, which also sets out how you can contribute.

Other linked consultations

The policy of the acquisition of communications data by public authorities has been subject to a number of public consultations over the last decade. These include:

- A consultation on the final phase of the implementation of the EU Data Retention Directive in 2008;
- A consultation on the first phase of the implementation of the EU Data Retention Directive in 2006;
- A consultation in 2006 on the statutory Code of Practice accompanying Part I, Chapter II of the Regulation of Investigatory Powers Act 2000 (RIPA), the legislation enabling public authorities to acquire communications data;
- A consultation in 2003 on the Code of Practice for the voluntary retention of communications data under the Anti-Terrorism, Crime and Security Act 2001 (ATCSA);
- A wider consultation on access to communications data by public authorities in 2003, seeking views on whether a number of additional public authorities should be entitled to acquire communications data.

The Home Office also launched, on 17 April 2009, a consultation seeking views on which public authorities should be entitled to have the ability to use powers regulated by RIPA, including the power to acquire communications data.

PART 1 – COMMUNICATIONS DATA AND HOW IT IS USED BY PUBLIC AUTHORITIES

1.1 What is Communications Data?

Communications data is information about a communication. It does not include the content of a communication. It can show when a communication happened, where it came from and where it was going, but it cannot show what was said or written.

For a given telephone call, communications data can include the telephone numbers involved, and the time and place the call was made, but not what was said. For an e-mail it might include the e-mail address from which the message was sent, and where it was sent to, but not the content of the e-mail.

The different types of communications data are described in Annex B.

The companies that currently provide us with communications services, such as telephone companies and internet service providers, use communications data to connect our calls and messages, provide us with the services we want and to charge us for the services we use.

The Data Protection Act 1998 (DPA) regulates the processing of personal data. The eight data protection principles provide the framework and the safeguards under which personal data is processed. The Regulation of Investigatory Powers Act 2000 (RIPA) and the Anti-terrorism Crime and Security Act 2000 (ATCSA) build upon these safeguards.

RIPA introduced a specific and transparent regime for the acquisition of communications data, fully compatible with the European Convention on Human Rights, providing strict safeguards, including independent oversight and means of complaint to an independent tribunal.

Prior to the ATCSA, the availability of communications data was dependent on the business practices of communications service providers. The ATCSA set out a clear regime for the retention of communications data by service providers for a limited and proportionate period (12 months) so that it could be subsequently accessed in a regulated way by public authorities under RIPA. The recent transposition of the EU Data Retention Directive into UK law provides further confidence that relevant communications data will be available when required by public authorities to protect the public. The EU Directive and other legislation relating to CD are described in more detail below.

Our European and other international partners have their own regimes for the use of communications data in the prevention, detection and prosecution of crime. Communications Data is universally regarded as a vital tool for national authorities. And the UK is at the forefront of developing a clear legislative framework which carefully regulates its use.

Further information on how the retention of, and access to, communications data is regulated in the UK is set out below.

1.2 Communications Data and Public Safety

Communications data plays a critical role in helping those public authorities whose responsibility it is to keep us safe to do their jobs. Assistant Commissioner John Yates of the Metropolitan Police has said that:

"The availability of Communications Data to investigators is absolutely crucial. Its importance to investigating the threat of terrorism and serious crime cannot be overstated.

Communications Data helps us save lives, provides us with opportunities to develop investigative leads, establishes the links between co-conspirators in the most serious of crimes, and assists us in the apprehension of fugitives from justice.

Finally, in a significant number of the most serious of cases, Communications Data provides the vital evidence that supports a successful prosecution of the offenders.

Without its continued availability, I am concerned that our ability to successfully investigate a wide range of crimes would be severely hampered."

Communications data is used by a number of public authorities specified by Parliament to protect the public. These public authorities include the security, intelligence and law enforcement agencies, and the emergency services. Data may also be obtained in more limited circumstances by local authorities when they are carrying out their statutory responsibilities to combat crime[1].

1. This consultation is about why and how communications data is collected, stored, and made available to public authorities. A separate public consultation was launched on 17 April 2009 dealing with the issue of which public authorities should be entitled to obtain communications data under the Regulation of Investigatory Powers Act, and for what purposes this should be allowed.

In 2007-8 there were 519,260[2] acquisitions of communications data under RIPA Part 1, Chapter II. Of this figure, a very small proportion (1,707 or 0.3%) involved acquisition of communications data by local authorities[3].

The Interception Commissioner confirmed that, "the intelligence agencies, police forces and other law enforcement agencies are the principal users of communications data" [4].

The Serious Organised Crime Agency has reported that, in 2006-7, lawful interception and communications data contributed to the recovery of £29m of criminal assets and stolen cash; 151 firearms being taken off the UK streets with the arrest of a number of gang members; some 830 arrests and the seizure of 3.5 tonnes of Class A drugs; and the rendering of assistance in 35 threat to life situations, leading to the prevention of a number of murders.

Communications data has four principal uses:

I. Building a picture of a suspect and a network of contacts

Communications data can provide a fast, secure and accurate indication of the activities and contacts of a suspected criminal or terrorist. Attributing these individuals to particular phone numbers or communications devices would be virtually

2. Interception of Communications Commissioner's Report 2007, paragraph 3.7, p8
3. Interception of Communications Commissioner's Report 2007, paragraph 3.26, p11
4. Interception of Communications Commissioner's Report 2007, paragraph 3.7, p8

impossible without using communications data. That data also allows the appropriate authorities to link a suspected terrorist or criminal to a network or gang to which they belong.

Communications data is therefore vital to counter-terrorism. It has played a significant part in almost all major Security Service investigations over the last decade.

Case study: a terrorist investigation

In June 2007 two separate attempted bomb attacks occurred in London's West End and at Glasgow airport.

The subsequent police investigation used communications data extensively to establish the chain of events that led up to the attempted bombings, and as evidence in the trial. Phone records showed that the two conspirators established contact in February 2007.

Mobile phones, that police established had been used by one of the conspirators before the attacks, were used as triggers for attempting to detonate the bombs in London's West End. This was later used as evidence to help to convict the bomber who survived his attack on Glasgow airport.

Case study: a drugs arrest

A search of a Dutch-registered vehicle recovered 40 kilos of heroin, 150 kilos of amphetamine, 556 kilos of ecstasy tablets and 15 kilos of ecstasy powder with an estimated street value of £19 million.

Eight mobile telephones were seized from the driver and the intended recipients. Combining physical evidence recovered from crime scenes with the associated communications data from these mobile phones enabled the investigating team to link the Sheffield based drug supplier and his brother and associates to the drugs seized from the lorry. This allowed further arrests and prosecutions to be brought.

Case study: protecting vulnerable children

A 10-month international police investigation into an online peer-to-peer network was coordinated by the Child Exploitation and Online Protection Centre (CEOP).

The investigation centred on a network used by paedophiles to request, trade and create hundreds of child abuse images.

Through the investigation 700 suspects were identified in 35 countries around the world. This was only possible through the use of communications data and covert internet investigative techniques.

As a result over 30 children were rescued from sexual abuse.

II. Providing evidence in criminal prosecutions

Communications data is used extensively as evidence in court. Bill Hughes, Director General of the Serious and Organised Crime Agency, states that:

"using communications data and intercept intelligence are key factors in over 95% of the most significant investigations directed at the Serious Organised Crime groups assessed as causing the most harm to the UK."

It is also used in most major terrorist trials.

Case study: the murder of Rhys Jones

On 22nd August 2007, Rhys Jones, an 11-year-old schoolboy, was shot dead in the car park of the Fir Tree pub in Croxteth, Liverpool. He was walking home from football practice when he became the innocent victim of a feud between two rival gangs.

Following a long and difficult investigation Sean Mercer was arrested, charged and subsequently convicted of the murder. Six other members of the gang were also convicted of assisting an offender and possession of prohibited firearms.

Communications data was used to attribute telephones to each of the offenders, demonstrate association at key times and place individuals at specific locations. It also showed that the telephones of the key offenders were in the Kirby area some twenty minutes after the murder – helping to establish that Mercer and other convicted associates attended business premises in order to burn the gunman's clothing and douse him in petrol to remove firearms discharge residue.

Communications data was essential to bringing the perpetrators to justice.

Case study: the murder of Holly Wells and Jessica Chapman

In 2002, during the investigation into the murder of Holly Wells and Jessica Chapman in Soham, Cambridgeshire, communications data from mobile phones exposed flaws in Ian Huntley's alibi. Data from Holly and Jessica's mobile phones showed that they had been in or very close to his house. Records of calls and text messages between Mr Huntley and his ex-girlfriend, Maxine Carr, also showed that she was in Grimsby when Mr Huntley killed the victims and that she deliberately misled the police over his whereabouts.

Case study: the murder of Sana Ali

In May 2007 Sana Ali was stabbed to death at her home address in Bury. Her husband had been having an affair with another woman, Harmohinder Sanghera, who was subsequently convicted of the murder.

The prosecution relied on the discovery of mobile phone location data which showed that Sanghera had travelled to Bury and back from her home address in Birmingham on the day the crime was committed.

Similar data also demonstrated to the jury that Sana Ali's husband was elsewhere at the time of the murder. Harmohinder Sanghera was later found guilty of murder.

III. Protecting vulnerable members of the public

Communications data is used daily to ensure that the emergency services can locate people who may be vulnerable to imminent harm:

- Emergency services use data to identify the location from where an emergency call has been made;
- And to identify the whereabouts of a missing person.

Case study: a kidnap investigation

In 1999, seven Chinese nationals were kidnapped in London after they had been smuggled into the UK, and ransoms demanded from their families in China.

One of the hostages had used the mobile phone of another Chinese migrant to call home the night before. Through communications data the Police were able to identify the destination number in China called by the UK mobile. They then asked UK communications service providers to check whether they had carried a call to that destination number since the man was kidnapped. One provider discovered that it had carried two calls within hours of the kidnap.

From the company's call data records the Police were able to tie the associated communications data to a number of other mobile phones and to fixed line telephones at a number of addresses. They were also able to identify the numbers being dialled in China, both those linked to the hostages' families and those linked to the gang members involved in collecting the ransoms. They were also able to identify the telephone numbers in The Netherlands of other gang members about to smuggle the next batch of illegal immigrants into the UK.

From this information the Police were able to put the locations in the UK identified from communications data records under surveillance, and provide the Chinese authorities with intelligence to put the gang extorting the ransoms there under surveillance too.

After nine days the hostages were rescued and 56 people involved in the conspiracy to kidnap were arrested, resulting in a combination of nine convictions, with many others being handed over to the immigration services.

Case study: a coastguard rescue at sea

In June 2008 a series of almost unintelligible mobile phone calls was received by Lincolnshire Police and Yarmouth and Humber Coastguards indicating that a yacht was in trouble in the North Sea. Yarmouth Coastguard requested communications data that enabled the caller's location to be estimated as two miles off Skegness.

Skegness All-Weather and Inshore Lifeboats were launched to assist and managed to find the yacht which had lost its mast, suffered propeller damage and was taking on water. Of the four people on board, one was very dehydrated from acute sea sickness.

The distressed crew members were taken aboard Skegness Lifeboat and returned safely to shore.

IV. Providing information which enables targeted interception of communications

Access to the content of any communication in transmission under warrant by the law enforcement and intelligence agencies must be personally authorised by the Secretary of State[5]. Analysis of communications data is an essential precondition of correctly targeted lawful interception. The law requires that interception warrants must describe the communications which are to be intercepted, for example by setting out the address, numbers or other factors that are to be used for identifying the communications that are to be intercepted. Without communications data that would not be possible.

1.3 The Collection and Retention of Communications Data today

I. Collection of data

Communications data is generated each time a call is made, or an e-mail sent. Much of this information is currently retained by the communications providers for their own business purposes. For example:

- It enables them to make sure a service is working properly and not being misused, and to bill their customers accurately where charges are based on usage. An itemised telephone bill shows us that we are only being charged for the calls that we have made;
- Companies also need to know when and how much their services are being used so that they can identify times of peak usage and what rates to charge. This enables them to manage their own networks appropriately to ensure that a service is available when customers want one;
- They may also want to collect information on usage so they know which other services their customers might be interested in. For example, a customer sending a large number of text messages whilst on a pay-as-you-go tariff on their mobile may be offered the chance to sign up to a pre-pay tariff with large numbers of free text messages;
- Companies also use this information to detect and investigate fraudulent use of their services and networks.

II. Retention of data

The Anti-terrorism, Crime and Security Act 2001 enabled the Secretary of State to issue a voluntary Code of Practice to communications service providers about the retention of communications data, where that data was either obtained or held for their own business purposes.

The Code of Practice approved by Parliament in November 2003 stated that communications data may be held by companies for 12 months expressly for the purpose of safeguarding national security [6]. Companies could retain data for longer than this if they needed to do so for their own business purposes.

5. Before issuing an interception warrant, the Secretary of State must believe the warrant is necessary in the interests of national security, to safeguard the economic well-being of the UK or to prevent or detect serious crime. Furthermore, the Secretary of State must also believe that the conduct authorised by the warrant is proportionate to what is sought to be achieved by carrying it out.

6. Or the prevention or detection of crime or prosecution of offenders where this related to national security.

More recently the EU Data Retention Directive (2006/24/EC) was adopted during the UK Presidency of the EU in 2005. The Directive provided for a more consistent approach across the EU to the retention of communications data and introduced mandatory requirements for retention of telephony and some internet-related data. The traditional telephony data requirements of the Directive were transposed into UK law by Regulations in October 2007. The UK minimum period for retention is 12 months. The remaining internet data requirements were transposed into UK law on 6 April 2009.

1.4 Access to communications data by public authorities and privacy: the safeguards

There is an important distinction to be drawn between the collection and retention of communications data by communications service providers and the acquisition of that data by public authorities in accordance with the requirements of the law. The vast majority of all communications data that is collected and retained today is never accessed by public authorities. The ability for public authorities to acquire stored communications data on a case-by-case basis to support investigations is also supported by strong safeguards so that access by public authorities to any of that data is tightly controlled.

I. The European Convention on Human Rights and the Regulation of Investigatory Powers Act

The acquisition of communications data by public authorities is regulated by RIPA. This legislation has a series of strict safeguards intended to ensure that the acquisition of communications data by public authorities is fully compliant with the European Convention on Human Rights.

Since much of communications data is personal information (on where people live or where they are using a mobile telephone, for example), its retention and subsequent access by public authorities interferes with an individual's right to respect for private and family life under Article 8 of the European Convention on Human Rights. Article 8(1) states that:

> *"Everyone has the right to respect for his private and family life, his home and his correspondence."*

Article 8 is, however, a qualified right which means that any interference with an individual's rights by the state is permissible so long as it is necessary (and not just reasonable) for a legitimate aim[7] and proportionate. Furthermore, the interference must have a clear legal basis.

RIPA put a regulatory framework around a range of investigatory powers to do just this. Specifically, Part I Chapter II of RIPA sets out a strict regime for the acquisition and disclosure of communications data:

- Data which has been retained can only be accessed by public authorities for a purpose stated in law;

7. A "legitimate aim" under article 8 of the ECHR includes the aims of national security, public safety, protection of the economy, prevention of crime, the protection of health or morals or the protection of the rights and freedoms of others.

- Data can only be obtained by a public authority specified in legislation, and only when authorised by a senior officer, holding a rank, office or position also specified in legislation;
- Data can only be obtained by a public authority when it is necessary in a given investigation;
- Data can only be obtained by a public authority when the interference with privacy that it will cause is proportionate;
- There is a statutory code of practice setting out how the legislation should be used and operated;
- There is external independent oversight of the application of the law; provided by the Interception of Communications Commissioner (currently Sir Paul Kennedy a former High Court judge);
- There is a right of complaint to the Investigatory Powers Tribunal if a member of the public believes that their data has been acquired unlawfully.

Communications data may only be acquired[8]:

- in the interests 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 (where a threat to this may threaten national security);
- 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's physical or mental health;
- to assist investigations into alleged miscarriages of justice;
- for the purpose of:
    i. assisting in identifying any person who has died otherwise 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, or
    ii. obtaining information about the next of kin or other connected persons of such a person or about the reason for his death or condition.

Public authorities that have requirements to gain access to communications data under RIPA must also be specified in the Act itself or designated in an order approved by Parliament. Authorisations to obtain communications data must be approved by a person holding a senior office, rank or position with the relevant public authority specified by Parliament to be able to do so.

8. The statutory purposes for which communications data may be accessed are listed in RIPA, Part I, Chapter II and in its associated statutory instruments:
Statutory Instrument 2003 – Number 3172: http://www.opsi.gov.uk/si/si2003/uksi_20033172_en.pdf;
Statutory Instrument 2005 – Number 1083: http://www.opsi.gov.uk/si/si2005/20051083.htm; Statutory Instrument 2006 – Number 1878: http://www.opsi.gov.uk/si/si2006/uksi_20061878_en.pdf

Restrictions also apply to the purposes (listed above) for which individual public authorities may acquire communications data and the types of communications data they may acquire. So, for example, a local authority can only obtain communications data if a senior individual with that authority (i.e. an Assistant Chief Officer or Assistant Head of Service level or equivalent) believes that it is necessary and proportionate to obtain the data and only then for the purpose of preventing or detecting crime. With respect to the different types of communications data, more detail on which is provided in Annex B, local authorities are only permitted to acquire subscriber information (e.g. registered name and address) and service usage information (e.g. numbers called from a telephone). They are not entitled to acquire traffic information – such as location information on a mobile phone.

II. Necessary and Proportionate

To satisfy the tests of necessity and proportionality, the authorising officer must first consider whether obtaining communications data is necessary for a statutory purpose. A police superintendent overseeing the work of an investigation team can only grant an authorisation if he believes that acquiring the data is necessary to prevent or detect crime. Furthermore, the designated person – in this case the superintendent – may not be directly involved in the investigation for which the authorisation is sought[9].

In determining proportionality, the authorising officer must consider whether securing the objective in a specific case, for example preventing a particular crime or apprehending an offender, justifies the level of intrusion into privacy caused by the acquisition of the communications data.

Only if the authorising officer believes that obtaining the communications data would be both necessary for a statutory purpose, and proportionate to what is sought by obtaining the data, can an authorisation be granted.

A code of practice, approved by Parliament, provides more detailed guidance to public authorities seeking access to data under RIPA. This code of practice is available online at:
http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf?view=Binary

III. Training for Communications Data Investigators

Communications data investigators – who work in law enforcement, intelligence agencies, and other public authorities – are normally highly specialised and undergo significant levels of training.

The single point of contact system (SPoC), extended beyond police to all relevant public authorities following the enactment of RIPA, created trained and accredited experts in each public authority who understand how to interpret the information that is held by communications service providers. This group, trained partially by industry to know what data is available to support investigations, helps to ensure effective working relationships between investigators and companies.

These communications data experts offer advice and assistance to investigating officers in their public authorities, making sure that they fully understand what

9. This additional requirement is imposed by virtue of Paragraph 3.11 of the Code of Practice on the Acquisition of Communications Data.

questions to ask, and what data to ask for. They can also provide advice on the least intrusive way to obtain the information that public authorities need, and the likely level of impact on privacy of asking a given question of a communications service provider.

IV. Further Safeguards and Oversight of RIPA

The process for obtaining communications data is rigorous. But there are also stringent statutory oversight arrangements to make sure the system works in practice. The Interception of Communications Commissioner keeps under review the powers and duties conferred by Chapter II Part I of RIPA. The person appointed as the Interception of Communications Commissioner must hold or have previously held a high judicial office. It is currently held by the Right Honourable Sir Paul Kennedy.

Oversight by the Interception of Communications Commissioner ensures that the authorisation procedures for obtaining communications data created by RIPA are applied lawfully and consistently. Part of the Commissioner's role is to protect people in the United Kingdom from any unlawful or unnecessary intrusion into their privacy.

The Commissioner has a team of inspectors who visit public authorities and examine the quality of decision-making and the use made of the data obtained, working to ensure that public authorities fulfil the requirements of the law set out in RIPA and its statutory Code of Practice. Inspections of public authorities take place throughout the year, and the Commissioner reports annually to the Prime Minister. His report is laid before Parliament.

These inspections look at a proportion of the cases where communications data has been acquired, and ensure that the authorising officer was of the necessary rank, and went through a full and thorough process of considering necessity and proportionality. The code of practice requires every relevant public authority to have a senior responsible officer who must be responsible for the integrity of the process to acquire communications data and, where necessary, to oversee the implementation of recommendations from inspections.

Furthermore, if any person believes that any of his communications data have been acquired unlawfully under RIPA, he is entitled to address a complaint to the Investigatory Powers Tribunal. This 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. The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of Government.

The Tribunal can be contacted through: http://www.ipt-uk.com/.

Regulation of Investigatory Powers Act 2000 - Acquisition and Disclosure of Communications Data.

Safeguards in brief:

- Any individual request to obtain communications data must be made by a "relevant public authority" specified by Parliament in accordance with Chapter II of Part I of RIPA;
- Each request must be necessary and proportionate in order to be granted;
- Each request can only be for one or more of the grounds set out in section 22(2) of RIPA (listed on page 17);
- The Interception of Communications Commissioner has a duty to keep under review the use of the statutory powers;
- The Investigatory Powers Tribunal has jurisdiction to examine claims or complaints relating to these powers.

V. The Data Protection Act 1998

Because communications data will often include personal data about the subscriber or user of a communications service, it is also subject to the provisions of the Data Protection Act 1998.

This Act works in two ways. First, it provides that anyone who processes personal information must comply with eight principles designed to ensure that personal information is:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in line with a person's rights;
- Secure;
- Not transferred to other countries without adequate protection.

Secondly, the Act provides individuals with certain qualified rights, including the right to find out what personal information is held about them by businesses and organisations, subject to certain exclusions set out in the Act, for instance where national security might be undermined. The Act also provides a framework to ensure that personal information is handled properly.

The Information Commissioner, appointed under the Data Protection Act, has various powers of enforcement and oversight, including:

- The power to serve enforcement notices on data controllers who have contravened or are contravening any of the data protection principles; and
- The power to assess whether personal data is being processed in compliance with the provisions of the Act.

PART 2 – THE NEW COMMUNICATIONS ENVIRONMENT

The communications industry is highly competitive and technologically driven. The UK is currently undergoing the most significant changes in communications since the development of the telephone. These changes are bringing significant benefits to the consumer. However, they will also have a profound effect on the ability of public authorities to use communications data to investigate crime and protect the public. If the Government does not act to keep up with these changes, the ability of public authorities to use communications data as they do now will be severely degraded.

2.1 The technological revolution

The extent of these changes was summarised in February 2008 by the cross-party Privy Council Review of the use of Intercept as Evidence[10]:

> *"Over the next several years the worldwide public telecommunications network will undergo a profound change. Hitherto almost all telephone networks have been circuit-switched: whenever a call is made the provider has set up a dedicated circuit (a combination of wires, channels within fibre optic, microwave or satellite trunks, and radio links to individual phones) which connects the callers. For as long as the call lasts the callers have exclusive use of this dedicated circuit. While other services than ordinary telephony (such as data) may be available, they are generally under the control of one of a small number of suppliers, who provide both the service and the underlying network, and do any necessary processing.*
>
> *Within the next 5 years we expect that most communications in the UK will instead be delivered using Internet Protocol (IP)[11]. [12]*

Communications data is as important a tool for investigating and prosecuting crime for our European and other international partners at it is for the UK. However, although other countries will also face the same challenges as the UK and will also suffer similar degradation in capability as technology advances, we will be one of the first to be affected by these changes. This is because:

- The UK telecommunications environment is one of the most dynamic in the world, due to deregulation;
- Many of the leading Western European countries still have dominant national fixed line companies, whereas the UK has a more 'open' market which encourages the spread and use of broadband;
- The UK's competitive communications market encourages companies to find new ways to offer new services and cut costs. BT, the largest network provider in the UK, is for example currently in the process of rolling out a nationwide network based on Internet Protocol.

The transition to communications based on Internet Protocol across the UK will have

10. The cross-party Privy Council Review of Intercept as Evidence was established in July 2007 to advise the Government on whether a regime to allow the use of intercepted material in court could be devised that facilitates bringing cases to trial while meeting the overriding imperative to safeguard national security

11. The international standard used for delivering material across the Internet.

12. Privy Council Report on Intercept as Evidence, page 27, paragraphs 107-8

five major consequences relevant to the collection of communications data:

- **There will be more ways to communicate**: the move towards IP, coupled with the rapid expansion and take up of new internet services means that there are now many more ways for people to communicate. In future, it is unlikely that the average person will solely use a fixed line telephone, or a fixed line and mobile. Already, many of us use e-mail, instant messaging, blogs, and social network sites in addition to these more traditional methods of communicating. We can expect this diversity in the way that people communicate to increase in future[13].

- **Companies may no longer need to keep as much information on the way customers use their services:** not all providers of communications services will continue to keep communications data as we know it now - records on who contacted who, when, and where. By making it cheaper and easier to provide services, Internet Protocol means that many companies have started to offer cheap, packaged or even free services. Some companies may no longer have any business need to keep information on service use by an individual subscriber.

- **Anonymisation will be an increasing feature of our communications:** until quite recently it was difficult to sign up to a new communications service without giving some personal information about the subscriber for identification, fraud prevention and billing purposes. But free services in particular mean there is less need for communications service providers to collect such information or to ensure it is reliable. The ability of any given person to have multiple communications identities for their fixed line numbers, mobile numbers, internet accounts and logins is making it easier for people to communicate anonymously.

- **More and more service providers will be based abroad:** a feature of the IP era is that any company, based in the UK or overseas, can make available communications services to UK consumers, using another company's physical network of cable and equipment. But communications services providers in the UK will very often have no business reasons to retain the third party communications data generated by services provided from overseas which cross their own networks. And overseas companies outside UK jurisdiction are not required to disclose data under RIPA and not required to retain the data under the EU Data Retention Directive.

- **Communications data is likely to be more fragmented in future:** people are more likely to use a greater range of communications services in future; and data relating to a single communications service might cross a number of different communications networks.

13. The OFCOM annual report 2008 confirms that people in the UK are moving towards new ways of communicating. In 2007, the average person in the UK spent 14 hours online per week – an increase of 6.5 hours since 2004. Half of all people using the internet in the UK use "social networking" websites such as Facebook or Bebo. Sixty percent of all households have broadband internet access. These all provide evidence that people in the UK are changing their behaviour, choosing to communicate through new technology rather than picking up the telephone. This evidence means that if we are to maintain public protection we need to change how we use communications data to do that

More communications services will be offered by different companies. For that reason, the data from one person's communications is more likely to be dispersed across a greater number of different companies and retained in different locations. With an increasingly competitive communications market, this trend will accelerate. Until now, data has been collected and retained by a relatively small number of UK firms about their own services. In the future it will be more difficult to identify the relevant company holding the data about a communication and that may include companies not based in the UK.

It is also possible that the data from a single service will be more fragmented. A web-based e-mail account, for example may be accessed using networks provided by many different UK companies – for example a Wi-Fi network provided in an airport or coffee shop, or a mobile phone network.

Case-study: communications diversity

The following example, included in the report of the independent cross-party Privy Council Review of Intercept as Evidence (2008), demonstrates the increasing diversity of communications services.

> *"Three friends Ian, Michael, and Stuart are planning a trip to the cricket. Stuart texts Ian from work to ensure he will be at his computer a little later to organise the trip. He then goes home and turns on his computer. He sends an Instant Message to see if Ian is online, which he is. Both then log onto their favourite Voice over IP (VoIP) package and begin discussing the trip.*
>
> *They quickly realise it would be easier if they could both see the fixture list, so Stuart e-mails to Ian a link to the cricket club's web-site. This fails, so instead he posts the link to a web forum they both use. They carry on their discussion and agree which match they wish to see. Michael is also online but does not have the same VoIP package so can't join in the conversation. However he and Ian are playing the same on-line computer game, and so use the in-game text-based chat function to discuss the details, Ian acting as a relay between Michael and Stuart.*
>
> *Finally all agree that Ian will buy the tickets. The others use an online bank (PayPal) to send the money to him. This in turn generates confirmation e-mails. So over the course of 30 minutes the three friends have used half a dozen different communications methods, not with any intention to conceal their activities but because it's a convenient and natural way to use the technology."*

2.2 The impact of these changes on the acquisition and use of communications data

The new communications environment will have an impact on how communications data is collected and retained, and on how it may later be used by public authorities:

- By increasing the number of ways that people communicate, changing technology is increasing the variety and amount of data that law enforcement and security and intelligence agencies need to pull together to understand the activities of a given criminal or a terrorist suspect. This therefore increases the scale of the challenge for the public authorities, as well as the complexity of their task;
- In addition to the greater scale of the challenge, the fragmentation of the data due to the wider range of services and the various networks such data can cross will hamper public authorities' investigations and operations. It will take longer to find and piece together the data needed to build up a picture on a suspect, or establish the whereabouts of a missing person;
- Because of the new ways of doing business (e.g. packaged or free services), companies may no longer retain the communications data which the police and intelligence agencies have used to great effect to help secure convictions and protect the public;
- And by giving access to a large number of services from different providers, which may or may not be provided from within the UK, internet protocol based communications mean that information needed by public authorities in the UK may not be kept in this country and may not be retained at all.

If public authorities are unable in the future either to gain access to the information they need, or to put this together to form a coherent piece of intelligence or evidence in similar timescales, then it will make investigation, whether of crime and terrorism or the location of vulnerable people, slower and more difficult, with obvious consequences for public safety as a whole.

Sir Stephen Lander, the Chair of the Serious Organised Crime Agency, has said:

> *"Any significant reduction in the capability of law enforcement agencies to acquire and exploit intercept intelligence and evidential communications data would lead to more unsolved murders, more firearms on our streets, more successful robberies, more unresolved kidnaps, more harm from the use of class A drugs, more illegal immigration and more unsolved serious crime overall."*

The Government has a responsibility to take action to ensure that the law enforcement and intelligence agencies' vital capabilities are not undermined in this way.

In practice, the Government has to find ways both (i) to ensure that all the potentially relevant data is collected and retained; and (ii) that it is done so in a way that allows public authorities to put together an increasing number of fragments to make a coherent whole.

Questions

Q1 **On the basis of this evidence and subject to current safeguards and oversight arrangements, do you agree that communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protecting the public?**

Q2 **Is it right for Government to maintain this capability by responding to the new communications environment?**

PART 3 – TACKLING THE CHALLENGE OF TECHNOLOGICAL CHANGE

Part 1 of this document described the critical role communications data plays in enabling the law enforcement, security and intelligence agencies and emergency services to do their jobs in protecting the public. It also described the detailed regulatory framework in place to prevent unnecessary intrusion in people's privacy, and the principles of necessity, proportionality, oversight and accountability which underpin it.

Part 2 set out the challenges of technological change, and how they will impact on the ability of public authorities to continue to use communications data as they do now – by reducing the proportion of communications data to which they can get access in the UK, and, through greater fragmentation, making it harder to use.

Part 3 looks at options for meeting these challenges and maintaining the capability which public authorities have at present and at safeguards and oversight.

3.1 The requirements

The fundamental requirement is for a system which, as far as possible, maintains our crucial communications data capability and, as is currently the case, balances the requirements of security and privacy in a way which commands public confidence. The more intrusive the methods, the more rigorous the safeguards need to be.

I. Privacy requirements

Any new regime must maintain the safeguards already provided for in law:

- Data which has been retained can only be accessed by public authorities for a purpose stated in law;
- Data can only be obtained by a public authority specified in legislation, and only when authorised by a senior officer, also specified in legislation;
- Data can be obtained by a public authority only when it is necessary in a given investigation;
- Data can be obtained by a public authority only when any interference with an individual's privacy is proportionate to the aims;
- There is external independent oversight of the application of the law;
- There is a right to complain to an independent tribunal if a member of the public believes that their data has not been acquired unlawfully.

II. Technological requirements

The two major consequences of technological change will need to be addressed: not all the communications data that public authorities may need will in future be collected and kept in the UK; and in the new IP environment data will be much more fragmented, making it much harder for public authorities to understand and use it.

a) Collection and retention

We need to ensure the collection and storage of communications data in connection with services accessed over UK communications networks, which is not already retained by the service providers for their business purposes. This would include third party data relating to internet-based services and communications services provided from outside the UK.

We also need to ensure that UK companies collect and store additional types of communications data about their own services, which are not included under the EU Data Retention Directive. This includes data that communication service providers do not generate or process about their services.

Data which has been collected will need to be retained by companies in the UK so that public authorities can continue to get access to it on a case-by-case basis under existing law (RIPA).

Some additional technical information (e.g. routing of internet communications services and/or domain name allocations) which is not required in the current traditional communications environment would also be required in future to help investigators understand the data around a communications event.

b) Processing the data to overcome fragmentation

Part 2 of the document described how communications data is now and will be in future distributed around an increasing number of companies – because individual users will be able to use a greater number of services and because even the data from a single service will be more fragmented. An overseas web-based e-mail account, for example, may be accessed using networks provided by many different UK companies. Fragmentation will make operations run by public authorities much slower: it will take longer to find and piece together the data needed to identify and build up a picture of a suspect, or establish the location of a missing person.

Automated processing of communications data by communications service providers once it has been collected, would make it possible for the data to be organised in a way that established the linkages between different pieces of data associated with, for example, the same phone, subscriber or number or a user ID.

In some cases data processing of this kind is already being done by UK communications service providers. Communications data associated with a single mobile phone may already be organised and collated by the company providing the service, to facilitate itemised billing.

The requirement would, therefore, be for a system run by communications service providers which organised and linked the data to make it easier to answer queries submitted by public authorities under an authorised request for communications data. So in practice, if a public authority needed to ask a relatively common question (such as what numbers a certain telephone has been in contact with in the last 24 hours), the answer would more likely be available in the timescales required.

This processing is potentially more intrusive than data retention itself; it would therefore require correspondingly strong and effective safeguards. The system could be designed so that a public authority had no visibility of how the data was linked together. The authority would only be provided with the limited data that was specified in an authorisation, which would have to be necessary and proportionate.

And of course, as is the case today, access to such information should not be possible without authorisation by a senior officer of a public authority.

3.2 A range of approaches

I. A single store

The Government has no plans to create a centralised database to store all communications data.

This would require the collection and retention of both communications data relating to the services offered by UK communications service providers, and also the additional third party data from services that UK communications service providers do not offer but that are carried over their networks.

This data would then be sent in near real time to a single location at which it would be stored. All this data would then be automatically arranged and organised, where appropriate, to enable subsequent lawful queries from public authorities to be answered quickly and effectively and in the timescales required, in accordance with the relevant safeguards.

This approach would have several advantages. It would be the option most likely to come close to maintaining the historic capability of public authorities in their use of communications data. It would be the most effective at delivering fast and efficient access in support of the law enforcement and intelligence agencies and emergency services; the least challenging technically to implement; and the cheapest to build and run.

However, this approach would also represent the most significant shift from the current system. Today, communications data is collected and retained by different companies in separate locations. Under this approach, all the data would be held together in one place.

The Government recognises the privacy implications in holding all communications data from the UK from a 12-month period in a single store. The Government therefore does not propose to pursue this approach.

There are therefore, only two further options, which are outlined in section iii) below ("A middle way?").

II. Doing nothing

This document has already set out the impact of changing communications technology on the way communications data is currently used by the law enforcement and other agencies. Failure to take action would leave only a limited and diminishing capability to continue to use communications data for the purposes for which it is currently used.

Nor is the use of communications data easily substituted by using other covert investigative methods, also regulated under RIPA. These techniques are more expensive, more manpower-intensive and slower. They cannot provide a record of a past event where communications data can. Communications data is generated by every communications event and it can therefore give an historical account of what happened to both criminals and victims. Other approaches would be much more intrusive, requiring physical or technical surveillance of a much larger number of people than is presently the case (or than current resources permit). Such techniques are also more high-risk and therefore less secure for both the public and the investigating agencies.

Jon Murphy, National Co-ordinator for Serious and Organised Crime for the Association of Chief Police Officers (ACPO) has said:

> *"The access to communications data is a fundamental investigative capability which is used daily by police officers to investigate serious crime and save lives, as well as being used routinely as a core element of the prosecution evidence in court. I could not contemplate a situation whereby law enforcement agencies were deprived of such crucial and compelling information."*

The Government therefore believes it would be failing in its duty to protect the public if it allowed the capability of public authorities to use communications data to degrade and made no effort to address it. **Doing nothing is not therefore an option.**

III. A middle way

The Government is therefore consulting on a range of "middle way" options that seek to balance the rights to privacy and security.

These options are all based on the model for collecting and retaining data that exists today: the communications service provider would collect the data and store it and allow access by the authorities on a case-by-case basis under RIPA. All the data would therefore continue to be distributed around and held by different communications providers.

As a first step, the Government would legislate to ensure that all the data that public authorities might need, including the third party data, is collected and kept in the UK. Communications service providers based in the UK would therefore continue to collect and retain communications data relating to their own services but also collect and store the additional third party data crossing their networks. This would therefore include communications data which does not come under the scope of the EU Data Retention Directive

All the data retained by the communications service providers would continue to be accessible on a case-by-case basis to public authorities, subject to the same rigorous safeguards that are now in place.

This option would put additional demands on industry, especially around the collection and retention of third party communications data not required for the business purposes of communications service providers. The Government is therefore actively seeking the views of industry on these proposals through this consultation.

This option would resolve the problem that some communications data which may be important to public authorities will not otherwise be retained in this country. However, it would not address the problem of fragmentation: as data is increasingly held by a wider range of communications service providers, it might take longer than it does at present to piece together data from different companies relating to one person or communications device. The current capability would therefore diminish.

To mitigate this problem the Government would require communications service providers not only to collect and store data but to organise it, matching third party data to their own data where it had features in common (for example, where it relates to the same person or to the same communications device). This would require additional legislation.

Organising data together would help to ensure that communications service providers would be better able to respond to a request from public authorities for all the data relevant to a specific communications device or subscriber. It would significantly decrease the turnaround time for requests and in life-threatening situations greatly help public authorities. In particular, where all the data that a public authority needed for an investigation was held by one communications service provider, this option would mean it was available quickly in a readily understandable form.

To maintain the capability set out in this document, the Government recommends taking the steps outlined above, specifically: that it legislates to ensure that all data that public authorities might need, including third party data, is collected and retained by communications service providers; and that the retained data is further processed by communications service providers enabling specific requests by public authorities to be processed quickly and comprehensively.

To assist us in complying with Better Regulation requirements this document is intended to stimulate discussion and elicit views both from those likely to be affected and any interested stakeholders. Any legislative provisions brought forward following this consultation will be accompanied by a fully developed and robust Impact Assessment measuring the impact on the public, private and third sectors. Specific impact tests required alongside the Impact Assessment, such as the construction of an Equality Impact Assessment, will also be addressed.

IV. Costs

The range of options would offer different levels of benefits to the public authorities, such as the law enforcement and intelligence agencies. Different options among the ranges available would also incur different levels of cost. Initial estimates of the implementation costs of the range of options discussed above are up to £2bn. This figure is a high level budgetary estimate of the economic costs[14].

As provided for in RIPA, the Government is required to ensure arrangements are in place to make reasonable contributions to communications service providers towards the costs incurred by them in complying with the Act's communications data requirements.

3.3 The Safeguards

This document proposes a way in which the current capability to store and access communications data can be maintained in the face of technological change. As far as possible the proposals reflect the arrangements which are currently in place.

14. These estimates cover all the options considered in this paper, except the 'Do Nothing' option".

The Government does not intend to pursue an approach which involves storing all communications data required by public authorities in a single place under Government control. Communications service providers will continue to collect and store data in their own data stores.

The regulations governing access to data will continue to be separate from the regulations governing its retention. As is currently the case, public authorities will only be able to acquire communications data on a case-by-case basis from service providers under the strict regulatory framework provided under RIPA. Public authorities will only ever access a very small proportion of the data that communications service providers will continue to collect and retain and will do so primarily in the context of a criminal investigation or threat to life.

In all of the options discussed in this document, the range of strict statutory safeguards, currently provided by RIPA (set out in Part 1) would continue to apply. In summary, these are that:

- Data which has been retained can only be accessed by public authorities for a purpose stated in law;
- Data can only be obtained by a public authority specified in legislation, and only when authorised by a senior officer, holding a rank, office or position also specified in legislation;
- Data can only be obtained by a public authority when it is necessary in a given investigation;
- Data can only be obtained by a public authority when the interference with privacy that it will cause is proportionate;
- There is a statutory code of practice setting out how the legislation should be used and operated;
- There is external independent oversight of the application of the law; provided by the Interception of Communications Commissioner (currently Sir Paul Kennedy a former High Court judge);
- There is a right of complaint to the Investigatory Powers Tribunal if a member of the public believes that their data has been acquired unlawfully.

Independent oversight would also continue to be provided by the Information Commissioner to ensure data protection principles were being observed.

Furthermore, an additional safeguard is provided through the offences contained in the Data Protection Act 1998 and the Computer Misuse Act 1990. These would ensure that appropriate penalties would exist for anyone who sought to either gain unauthorised access to ("hack") or modify any communications data held on a computer system, and that penalties also existed for those who tried to obtain or disclose, or procure the disclosure of, communications data in such a system without a lawful authorisation or notice under RIPA[15] .

15. Under the Computer Misuse Act 1990 (as amended), the maximum penalty for the unauthorised access offence ("hacking") is currently 2 years' imprisonment, on conviction on indictment. Under the same Act, the maximum penalty for the unauthorised access offence with the intent to commit further offences (e.g. to gain access to sensitive information held on the computer with a view to blackmailing the person to whom that information related) is 5 years imprisonment, on conviction on indictment. Unauthorised acts with intent to impair the operation of a computer carry a maximum penalty on conviction on indictment of 10 years' imprisonment. Unlawful obtaining or disclosure of personal data is an offence under the Data Protection Act 1998, attracting a fine on conviction on indictment.

In addition to these safeguards, a statutory limit would be imposed on the duration for which additional data collected by communications service providers could be retained. This would relate to the data that service providers were required to collect and keep by law from services that were not offered by them, but which crossed their networks. The statutory limit would be set at 12 months, in line with the voluntary code approved under the ATCSA and in line with the UK transposition of the EU Data Retention Directive.

This period might need to be extended in specific cases in certain circumstances – where the data was needed for specific legal proceedings. Any such exemptions would also have to be set out in primary legislation. After the retention period all retained data would be destroyed in line with data protection principles.

With regard to technical and physical safeguards, the confidentiality and integrity of communications data throughout the system will be ensured by working with communications service providers, suppliers and designated public authorities. Physical and procedural security will ensure no single point of vulnerability.

Procedurally, compliance with the HMG Security Policy Framework, the obligations of the Data Protection Act and applicable guidance from the Information Commissioner's Office will be enforced. Acquisition of communications data will be limited to those who have a need to know following properly authorised requests. Information will be destroyed once its designated period of retention has expired.

Physical and technical security safeguards will include:

- physical and system access controls to prevent unauthorised access, amendment or removal of data;
- accredited secure communications networks for the transport of sensitive information;
- encrypted stored data where appropriate;
- security monitoring and audit to ensure compliance and to detect any attempts to breach security.

Built-in management information systems will aid external scrutiny such as that provided by the Interception and Information Commissioners.

PART 4 – CONCLUSION

The Government acknowledges that this is a sensitive area, and one about which the public is rightly concerned. Balancing privacy and security requires detailed and considered thought.

The Government is clear that it must act in the face of technological changes which would lead to a reduction in the capability of public authorities to use communications data. To do nothing would lead to a greater proportion of crimes going unsolved, and more cases in which public authorities could not protect or prevent people from coming to harm.

The challenge is to find a model which strikes the right balance between maximising public protection and the ability of the law enforcement and other authorities to do their jobs to prevent and detect crime and protect the public, and minimising the intrusion into our private lives.

Questions

Q3 **Do you support the Government's approach to maintaining our capabilities? Which of the solutions should it adopt?**

Q4 **Do you believe that the safeguards outlined are sufficient for communications data in the future?**

ANNEX A

QUESTIONS

The Government would welcome responses on the following questions:

Q1 **On the basis of this evidence and subject to current safeguards and oversight arrangements, do you agree that communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protecting the public?**
Found on page 22

Q2 **Is it right for Government to maintain this capability by responding to the new communications environment?**
Found on page 22

Q3 **Do you support the Government's approach to maintaining our capabilities? Which of the solutions should it adopt?**
Found on page 30

Q4 **Do you believe that the safeguards outlined are sufficient for communications data in the future?**
Found on page 30

If there are any other additional comments that you would like to make, and are unable to make that comment in response to these questions, please forward these to:

Nigel Burrowes
Communications Data Consultation
Room P.5.37
Home Office
2 Marsham Street
London SW1P 4DF

Or by e-mail to: communicationsdataconsultation@homeoffice.gsi.gov.uk

ANNEX B

COMMUNICATIONS DATA IN DETAIL

Communications data does not include the contents of any communication. The acquisition and disclosure of communications data is currently regulated by the Regulation of Investigatory Powers Act 2000. Communications data as defined by this Act means:

- information about communications (traffic data, section 21(4)(a));
- information about the use of communications services (service use data, section 21(4)(b)); and
- information about communications service users (subscriber data, section 21(4)(c)).

Traffic Data

Traffic data is data that is comprised in or attached to a communication for the purpose of transmitting the communication and which 'in relation to any communication':

- identifies, or appears to identify, any person, equipment[16] or location to or from which a communication is or may be transmitted;
- identifies or selects, or appears to identify or select, transmission equipment;
- comprises signals that activate equipment used, wholly or partially, for the transmission of any communication (such as data generated in the use of carrier pre-select or redirect communication services or data generated in the commission of, what is known as, 'dial through' fraud);
- identifies data as data comprised in or attached to a communication. This includes data which is found at the beginning of each packet in a packet switched network that indicates which communications data attaches to which communication.

Traffic data includes data identifying a computer file or a computer program to which access has been obtained, or which has been run, by means of the communication – but only to the extent that the file or program is identified by reference to the apparatus in which the file or program is stored. In relation to internet communications, this means traffic data stops at the apparatus within which files or programs are stored, so that traffic data may identify a server or domain name (web site) but not a web page.

16. In this code equipment has the same meaning as 'apparatus', which is defined in section 81(1) of the Act to mean 'any equipment, machinery, device, wire or cable'.

Examples of traffic data 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 Internet Protocol 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);
- web browsing information to the extent that only a host machine, server or domain is 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).

Service Use Information

Data relating to the use made by any person of a postal or telecommunications service, or any part of it, is widely known as 'service use information'.

Examples of data 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.

Subscriber Information

Subscriber information relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service. 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:

- 'subscriber checks' (also known as 'reverse look ups') such as "who is the subscriber of phone number 012 345 6789?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- 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 CSP, 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 save where the requirement for such information is necessary in the interests of national security).

Printed in the UK for The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID 6112445 04/09

Printed on Paper containing 75% recycled fibre content minimum.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone Fax & E-Mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/ General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: http://www.bookshop.parliament.uk

TSO@Blackwell and other Accredited Agents

Customers can also order publications from
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401

ISBN 978-0-10-175862-8

9 780101 758628