Home Office

PROTECTING THE PUBLIC IN A CHANGING COMMUNICATIONS ENVIRONMENT

Summary of Responses to the 2009 Consultation Paper

Contents

A. INTRODUCTION 3

B. SUMMARY OF RESPONSES 4

C. OTHER AREAS RAISED DURING CONSULTATION 14

D. CONCLUSION 16

ANNEX A: GOVERNMENT ACTIVITY DURING CONSULTATION 17

ANNEX B: LIST OF RESPONDENTS 19

ANNEX C: BACKGROUND ON COMMUNICATIONS DATA 21

ANNEX D: CASE STUDIES ON COMMUNICATIONS DATA 23

A. INTRODUCTION

On 27 April 2009 the Home Office launched a three month consultation on "Protecting the Public in a Changing Communications Environment".

Communications data – the who, where, when and how of a communication, but not its contents – plays a vital role in protecting the public. In situations such as kidnappings, responding to emergency calls, investigating serious crime or preventing terrorism, it can save lives. The public is therefore entitled to expect that it will be used effectively.

Rapid technological change in the communications industry is posing increasing challenges to the use of communications data to protect the public. If these challenges are not addressed, the public will lose protection to which they have become accustomed and to which they are entitled.

The consultation paper set out the Government's proposals to ensure that communications data can continue to be used effectively. It also explained the Government's continuing determination to ensure that communications data is only used when it is necessary and proportionate. Finally, it invited readers to respond to the Government's proposals.

The text of the paper is at:

http://www.homeoffice.gov.uk/documents/cons-2009-communications-data?view=Binary

The Home Office asked the following questions:

1. On the basis of this evidence [provided in the paper] 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?
2. Is it right for the Government to maintain this capability by responding to the new communications environment?
3. Do you support the Government's approach to maintaining our capabilities? Which of the solutions should it adopt?
4. Do you believe that the safeguards outlined are sufficient for communications data in the future?

221 responses were received. This document summarises the responses and explains the Government's position.

Any queries about this document should be made to:

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

Or

E-mail: communicationsdataconsultation@homeoffice.gsi.gov.uk

B. SUMMARY OF RESPONSES

The 221 respondents comprised 167 members of the public and 54 organisations including communications services providers, industry bodies, public authorities and campaign groups. A list of the respondents is provided in Annex B.

90 respondents did not address the questions asked but objected generally to the paper, almost invariably on the grounds of opposition in principle to any sort of surveillance. The percentages given below (in relation to each of the questions asked) therefore only relate to the 131 responses which provided a positive or negative response to the consultation's specific questions. Where the percentages do not add up to 100% the balance is due to answers that addressed the specific question without being clearly negative or positive.

The main themes to emerge in responses were:

- widespread (but not unanimous) recognition of the importance of communications data in protecting the public;
- widespread appreciation of the challenges which rapidly changing technology poses;
- some support for the Government's proposed ways of meeting these challenges;
- but also concerns about whether the Government's proposals would be technically feasible or would impose unreasonable burdens on industry;
- some concern about whether the assessment of the balance of costs and benefits of the Government's proposals was realistic;
- a desire from a number of respondents for greater clarity on why existing legislation and regulations were not capable of meeting the Government's stated requirements;
- but also a recognition, particularly amongst those involved in the communications industry, that current legislation and regulations relating to the collection, retention and processing of communications data, particularly third party data, would soon need to be updated in light of changing technology;
- concerns about protecting communications data, where both privacy and commercial interests were engaged; and
- calls for more judicial involvement, and greater visibility and public awareness of existing oversight mechanisms, in order to improve public confidence in the way public authorities use communications data to protect them.

An examination of the responses to each question asked in the paper, and some of the wider comments raised, follows.

OTHER CONSULTATIONS

The Home Office had a parallel consultation on the range of public authorities able to use different investigatory techniques, including accessing communications data, under the Regulation of Investigatory Powers Act 2000 (RIPA). The consultation document 'Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice' can be found at:

http://www.homeoffice.gov.uk/documents/cons-2009-ripa?view=Binary

The Summary of Responses to that consultation is also published on the Home Office website.

Question 1: 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?

YES

59% of respondents agreed that communications data was at least an important, and in some cases a vital, tool for public authorities. Support for this position was particularly strong among those with a specific interest in the use of communications data on behalf of the public, including relevant public authorities and victims groups such as Support After Murder and Manslaughter. All of the law enforcement and emergency services that responded stated that communications data was vital in allowing them to protect the public:

"Communications data provides pivotal and compelling evidence in most court cases that involve allegations of serious crime. As well as often being primary evidence, it is also used to corroborate other evidence. It helps to establish the truth and to prove or disprove a defendant's involvement in the matter being investigated." [Police Superintendents Association of England and Wales]

"Communications data, which does not include the contents of communications, has proved valuable for law enforcement purposes over many years. Lawful access to communications data allows investigators to identify suspects and their 'hidden' means of communication, trace their criminal contacts, establish hierarchical relationships between conspirators, place them in specific locations at specific times, identify their banks and those engaged in laundering their criminal finances and assets both in the UK and abroad, and can confirm or disprove suspects' alibis." [Association of Chief Police Officers]

"We are well aware that collecting such data has a key role in a number of very important child protection investigations by enabling the police to identify vital information and leads." [Children's Charities' Coalition on Internet Safety]

"The need to collect and retain historical CD [communications data] is taken as a given – the justification for doing so rests on current practice and examples of successful prosecutions." [Liberty]

Many respondents welcomed reassurances that the Government's proposals related only to communications data, and not to the contents of communications.

Some respondents thought the Government's case could have been made stronger by including a wider range of case studies to reflect the breadth of work necessary to protect the public.

Whilst most respondents agreed that communications data was an important tool for the law enforcement and security and intelligence agencies, some did not believe that other public authorities had a necessary and proportionate need to access such data.

NO

18% of respondents answered 'no' to question 1. Some respondents argued that the proposals were an attempt to extend the use of what they believed was "terrorism legislation" beyond its scope:

"No. The argument that CD is vital is spurious". [member of the public]

"No. In some circumstances communications data is useful, and … the law enforcement agencies have made use of communications data to tackle crime. However, that does not make it vital." [member of the public]

Some respondents were opposed to any form of what they regarded as 'surveillance', including the use of communications data. Further, some respondents believed that the Government would be 'monitoring' all communications.

GOVERNMENT'S POSITION

As the consultation paper made clear, the Government believes that communications data is a vital tool for public authorities who protect the public.

The Government's proposals relating to communications data have been widely misrepresented.

Neither the current legislation relating to the use of communications data, nor the Government's proposals for the future, are limited to terrorism. RIPA, which sets out the main framework through which public authorities access communications data, is not terrorism legislation. Instead, it regulates a number of investigatory techniques which are used by a wide range of public authorities to protect the public. It provides that a public authority may only acquire communications data for purposes such as preventing and detecting crime, and protecting public health or public safety. But RIPA makes it clear that communications data, like the other techniques which it regulates, should only be used if it is necessary and proportionate to do so. This is consistent with Article 8 of the European Convention on Human Rights.

As the consultation paper also stated, the Government is clear that communications data will continue to be retained by the communications services providers, not by Government. Public authorities seeking access to that data will continue to need to seek senior officer approval to do so. These requests must be compliant with RIPA.

Further information on safeguards relating to the use of communications data is included in the section covering question 4 of the consultation.

Question 2: Is it right for Government to maintain this capability by responding to the new communications environment?

YES

53% of respondents said that the Government should act to maintain the capability of public authorities to use communications data to protect the public. There was widespread understanding that rapidly changing technologies would have an impact on current communications data capabilities. This led a majority of respondents to agree that it was right for the Government to respond to the new communications environment. Some respondents believed the Government would be failing in its duty if it did not ensure that the security, intelligence and emergency services could continue to protect the public by using communications data:

"Yes. As the means by which people communicate with each other changes, so the government must change the way law enforcement agencies gather information." [member of the public]

"If the Government does not maintain the capability or capacity for the police to determine, when necessary and proportionate and in accordance with law, as to who has communicated with whom and when, the police service will face a fundamental breakdown in our ability to function in, what is now termed, the communications age." [Association of Chief Police Officers]

"If we lose our existing capabilities, it cannot be replaced simply by investing in other conventional policing techniques. If the current capability is lost or significantly diminishes, then lives will be lost unnecessarily, a large number of the most serious crimes will remain undetected, and those responsible will remain free to commit further crimes and cause more harm to society. We therefore endorse the approach outlined by the Government in the public consultation document." [Police Superintendents Association of England and Wales]

NO

22% of respondents answered 'no' to question 2. Some respondents disagreed in principle with all forms of what they regarded as 'surveillance'. They therefore did not agree that it was right for the Government to maintain the capability of public authorities to use communications data to protect the public. A small minority perceived threats, for example from terrorism, to be negligible or exaggerated. They stated that they were prepared to accept the risks arising from such threats rather than accept the Government's proposals to maintain the capabilities necessary to counter them. Some respondents believed the Government was seeking to extend or expand, rather than maintain, capabilities:

"No. The Government should not require anyone to keep records on communications." [member of the public]

"No; the only satisfactory solution would be 'do nothing'." [member of the public]

GOVERNMENT'S POSITION

Communications data is fundamental to many investigations and it would not be possible to achieve the same results using other investigatory techniques, such as covert surveillance. These other techniques can be more resource-intensive, time-consuming and intrusive than the use of communications data.

Most importantly, these other techniques cannot be used retrospectively. They cannot assist in reconstructing past events. By contrast, communications data is generated by every communications event. It can therefore allow investigators to understand the past activities of criminals – and in some cases their victims. The use of communications data to protect the public is invaluable and irreplaceable.

The Government has proposed new measures, which would include primary legislation, to ensure that the overall capability of public authorities to protect the public is maintained. The Government's challenge is to maintain investigative capability to protect the public through the use of communications data as technology develops. To do this against today's rapidly changing and increasingly diverse communications environment means that the Government needs to develop the ability of public authorities to use communications data from

a wider range of technologies in order to provide the same level of public protection as in the past. Continuing to use communications data as technology changes can be less intrusive than other methods of maintaining current levels of investigative capability, e.g. increased surveillance. The Government will ensure that the use of communications data continues to be proportionate and reasonable, with proper accountability, safeguards and oversight.

Question 3: Do you support the Government's approach to maintaining our capabilities? Which of the solutions should it adopt?

YES

29% of respondents supported the Government's approach, although a higher proportion welcomed the Government's statement that it did not intend to create a single store for all communications data.

The respondents who supported the Government's proposed approach believed it to be an appropriate and proportionate means of ensuring that, as far as possible, the capability to use communications data to protect the public is maintained:

> *"We consider that any invasion of privacy must have a legitimate purpose, be necessary and proportionate and have effective safeguards. The Government's "middle way" option appropriately seeks to balance individuals' rights to privacy with security considerations."* [Crown Prosecution Service]
>
> *"The Information Commissioner welcomes the fact that the consultation document rejects the proposal that all of the additional data collected be kept in a single database, held by the Government or a central agency. The Home Office recognise that a single database would be a step too far and appreciate that privacy concerns are engaged by the increasing collection and retention of communications traffic data."* [Information Commissioner's Office]
>
> *"Please understand that while I have these concerns, I do feel that the proposed option is still superior to the 'do nothing' or 'single database' solution proposed."* [member of the public]

Technology providers considered that the Government's proposed approach could lead to a viable solution, although for some it could be challenging. It was suggested that options for delivering the approach should be trialled with sample providers and within a model office environment in order to develop best practice. This category of respondents also considered that there were few technological barriers to the Government's proposed solution. The adoption of common standards and procedures was recommended to simplify implementation and to keep overall costs down. The current requirements for data security outlined in the EU Data Retention Directive and fully transposed into UK law by the Data Retention (EC Directive) Regulations 2009 were strongly supported by a security software company, which recommended that similar requirements be included in any new legislation.

NO

38% of respondents opposed the Government's approach. The majority of these thought the Government should 'do nothing'. This was because they objected to all forms of what they regarded as 'surveillance':

> *"The government should not require anyone to keep records on communications."* [member of the public]

Several respondents did not feel the case had yet been made for the collection and retention of communications data to the extent proposed. They said there should be more discrimination about what data is retained:

> *"Based on the evidence presented in the consultation, and further documentation available to us, the Information Commissioner believes that the case has yet to be made for the collection and processing of additional communications data for the population as a whole being relevant and not excessive."* [Information Commissioner's Office]

Some respondents who recognised it was important to maintain our communications data capability (in response to question 2) nonetheless supported the "do nothing" option. This was on the basis that they believed that either existing legislation, in particular the Data Retention (EC Directive) Regulations 2009, would suffice, or that other investigative powers should be used instead.

Although there was very limited support for the option of creating a single database for all communications data (an option the Government had already rejected), some respondents suggested such a database would be the most effective way of processing and protecting data.

Communications Service Providers raised concerns about how new proposals might potentially impact on their businesses. They noted:

- the importance of the Government continuing to compensate service providers for additional costs arising out of the retention of communications data and responding to requests for that data from relevant public authorities;
- the importance of ensuring that additional requirements would be reasonable and technically feasible;
- the need for the Government to provide technical assistance in some respects;
- the need for new proposals to be consistent with the European Convention on Human Rights and relevant EU legislation and requirements; and
- that new proposals might lead to additional demands for disclosure to third parties.

Communication service providers also considered that communications data should only be disclosed under the provisions of RIPA and not through any other existing statute or legal power.

GOVERNMENT'S POSITION

The Government does not believe that relying on existing legislation, in particular the 2009 Regulations transposing the EU Data Retention Directive (2006/24/EC – 'the DRD') into UK law, will maintain existing communications data capabilities. The purpose of the DRD was to provide a more consistent approach across the EU to the retention of communications data. The DRD does not meet all requirements in two respects:

- not all communication data is covered in the scope of the Directive, for example communications data relating to web chat; and
- increasingly, companies that run the networks have no contractual relationship with the communications service being used. One company might provide the broadband network service, whilst a separate company, which might be based abroad, provides an email account. This is a 'third party' relationship; and the company providing the broadband access has no responsibility under the DRD to retain third party data.

The Government believes that it would be irresponsible to retain only certain sets of communications data, as proposed by some respondents. Criminals do not limit themselves to particular communications services or media. Victims should be able to have confidence in the ability of the police and other agencies to protect them, regardless of which type of communications service or device was used by those who harmed them. The Government therefore believes it would be detrimental to the public interest to seek to identify categories of communications data which should not be retained.

As the consultation paper confirmed, the vast majority of communications data collected and retained by communications service providers is never accessed by public authorities. This will remain the case.

The Government acknowledges that the use of different statutory frameworks, for example the Social Security Fraud Act 2001, to access communications data may be undesirable. It is arguable that communications data should only be obtained through RIPA, which combines a robust regulatory regime which requires compliance with human rights, with separate independent oversight and redress mechanisms and a fair system of reimbursement to communications service providers. We therefore propose to review all mechanisms by which public authorities can obtain communications data to see if a single means of authorised access through RIPA would be practicable.

The Government's proposed approach is based on the current data retention system, in which communications service providers own and manage communications data generated within their infrastructure.

Whilst recognising the challenges, the Government is confident its proposed solution is technically feasible and will continue to work with communications service providers in developing it.

Question 4: Do you believe that the safeguards outlined are sufficient for communications in the future?

YES

26% of respondents believed the safeguards outlined to be measured and proportionate. The majority of those who use communications data to protect the public already, and are familiar with the full range of safeguards currently in place, agreed that the safeguards outlined were appropriate:

"We believe that the current safeguards are sufficient and the process for the acquisition of communications data ensures that only where proportionate and necessary are rights to privacy invaded. Were additional levels of bureaucracy to be implemented, the ability to access communications data in a timely operational manner would be impeded and its value and use in investigations reduced." [Child Exploitation and Online Protection Centre]

"In all cases, and before [HMRC] acquires any data, a senior officer will consider if the requirement to disclose data is necessary and proportionate and whether there is any risk of intrusion into the privacy of individuals who are not involved in the criminal activity under investigation. To further ensure objectivity, the authorising officer is not permitted to be directly involved in the investigation. Authorising Officers are provided with specific training in this role to ensure that the highests standards are maintained. HMRC is subject to regular inspections by the Interception of Communications Commissioners Office (IOCCO) to ensure full compliance with RIPA and the Code of Practice". [Her Majesty's Revenue and Customs]

"Broadly the safeguards seem principled and proportionate. For openness, a disclosure describing numbers of requests, successful uses and failures would be very useful." [The Statistical Society]

NO

50% of respondents did not believe the safeguards outlined were adequate. Some respondents, particularly amongst members of the public, were concerned that the proposals meant all communications data would be monitored, and would allow for disproportionate and unnecessary 'fishing expeditions' for data:

"The Government is going too far, and when the terrorists etc. know that you are monitoring all internet communications they will use something else, but you will not stop monitoring innocent and lawful activities". [member of the public]

"Much more worrying is that this is part of a police state network of spying on individual citizens". [member of the public]

Independent authorisation of access to communications data was the most common suggestion from those who were not satisfied with the existing safeguards:

"I am deeply concerned that the government seems entirely happy for RIPA to allow everyone from the police to local authorities to access my communications data (everything from who I phone to what websites I look at) without a warrant or any judicial oversight". [member of the public]

There was widespread concern about the safety and security of communications data which would be retained and the potential for abuse. For some, the fact that under the Government's approach communications data would continue to be retained by communications service providers and not Government did not allay this concern. Some respondents thought that existing offences under the Data Protection Act 1998 and the Computer Misuse Act 1990 might not be sufficient.

Communications service providers considered that safeguards should continue to include statutory restrictions on who can access communications data and ensure that third party communications data relating to applications and services provided by third parties and retained by communications service providers could not be used for commercial purposes in an anti-competitive way. They were also concerned that there should be clarity on how Data Protection Act 1998 requirements on security, reliability and legal responsibility with regard to the lawful processing and control of communications data would be met.

Some respondents believed that the current oversight mechanisms should be more visible. They emphasised that they should be properly resourced for any new responsibilities.

GOVERNMENT'S POSITION

The Government is clear that the use of communications data to protect the public should be subject to a comprehensive range of safeguards to ensure that privacy is protected appropriately. RIPA contains strict safeguards which would make disproportionate and unnecessary 'fishing expeditions' unlawful. Under RIPA:

- data which has been retained can only be acquired by public authorities for a purpose stated in law;
- data can be obtained only when authorised by a senior officer, holding a rank, office or position 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 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 exercise of the relevant powers; provided by the Interception of Communications Commissioner, who must hold, or have held, held high judicial office; and
- 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.

These safeguards mean that only applications for communications data which are related to specific investigations involving specific data will be capable of satisfying the tests of necessity, proportionality and legitimate aim. Broad enquiries which amount to no more than fishing expeditions attempting to uncover or predict crimes will fail the tests set out in RIPA and will remain unlawful. It is not therefore the case that the proposals in the consultation will mean that the Government is monitoring all internet communications or even acquiring access to all communications data.

In addition to the RIPA safeguards, communications service providers and public authorities must comply with the data protection principles in the Data Protection Act 1998. These apply to all personal data, including most communications data, with respect to which they are the data controllers. This statutory regime applies to the processing of communications data held by communications service providers, and by public authorities when they have acquired communications data under RIPA.

The Information Commissioner, appointed under the Data Protection Act 1998, 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 the data is being processed in compliance with the provisions of the Act.

The Government is seeking to strengthen these powers by bringing into force provisions in the Criminal Justice and Immigration Act 2008 and through the data protection clauses in the Coroners and Justice Bill, which is currently before Parliament. Additionally on 15 October 2009, the Ministry of Justice launched a consultation on exercising the power to provide for custodial sanctions for those found guilty of knowingly or recklessly obtaining, disclosing, selling or procuring the disclosure of personal data without the consent of the data controller. These are all offences under section 55 of the Data Protection Act. The consultation closes on 7 January 2010. A link to the consultation documents can be found at http://www.justice.gov.uk/consultations/misuse-personal-data.htm.

The Government will continue to work with communications service providers to address their concerns

about how the Data Protection Act 1998 will apply to them, and to ensure that data retained is not abused, as proposals relating to communications data are developed.

As the existing safeguards make clear, the value of independent oversight of the way in which public authorities access communications data under RIPA is not in question. The Government believes, however, that any requirement for authorisation by magistrates in relation to all acquisition of communications data could seriously impair the effectiveness of the techniques in question without bringing any real benefits in terms of protecting privacy. Magistrates are not best placed to apply the test of necessity and proportionality because they are not familiar with the operational parameters within which investigations are carried out. Nor would a system of authorisation by magistrates be compatible with the speed and flexibility which are frequently necessary to ensure that these techniques can be used effectively.

The Government will continue to ensure that resource requirements identified by the Interception of Communications Commissioner are met. The Commissioner reports annually to the Prime Minister on the carrying out of his oversight responsibilities and his report is laid before Parliament and published. His latest report for 2008 was published on 20 July 2009.

C. OTHER AREAS RAISED DURING CONSULTATION

Costs and Business Impact

The consultation paper provided an initial estimate of up to £2bn over 10 years for the implementation costs of the range of options discussed in the paper. This figure is a high level budgetary estimate of the economic costs. As proposals are developed, all costs will be subject to the normal rules on Government procurement. They will be assessed in terms of value for money and affordability. Further, the Government will work with communications service providers to develop solutions which minimise potential disruption to their business.

Any legislation brought forward will be accompanied by a full impact assessment.

Technical Issues

Encryption/anonymisation

The Government acknowledges that the use of encryption technologies is likely to change over time. Work will continue to identify the impact that encryption is likely to have on the ability of public authorities to obtain and use communications data. To that extent, trends will be monitored and adjustments made accordingly.

Where appropriate and necessary, RIPA Part III provides a legal framework under which authorised public authorities are able to issue notices requiring their recipients to supply encrypted material in an unencrypted form or to provide the relevant public authority with the means of decrypting the material.

The anonymity of the user of a communications device or account can be a considerable problem for investigating officers. Where a device or account cannot be linked to a named individual through the use of communications data, other methods have to be used. However, this communications data is still of considerable value in criminal investigations, and, where it is possible through other methods to link the device to a person, in providing evidence for prosecutions.

Deep Packet Inspection (DPI)

DPI is a term used to describe the technical process whereby many communications service providers currently identify and obtain communications data from their networks for their business purposes. Such processes may also be used to carry out lawful interception.

A number of respondents appear to have been misled by speculation that any use of DPI for Government purposes will blur the distinction between the interception of the content of a communication (as defined by RIPA) and retaining and processing communications data. RIPA provides that a person intercepts a communication in the course of its transmission by means of a telecommunication system if he modifies or interferes with the system, or monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system "as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication" (section 2(2) RIPA). Regardless of the technical solutions that might be used today or in the future to obtain communications data, interception, as defined by RIPA, will remain lawful only for a limited purposes and by a limited number of public authorities under a warrant issued by the Secretary of State and for certain other strictly defined purposes.

The current definitions for communications data and interception of communications will continue to be appropriate for new methods of communication. There is a recognition, however, that the evolution of new communications technologies will require ongoing work to ensure that communications data can be unambiguously separated out from the content of communications. By way of comparison, whilst layering of a number of internet protocols in internet communications can be complex, such layering can also exists in telephony. Any issues relating to telephony layering have long been overcome, ensuring the communications data can be separated from content.

Legal Framework

Compatibility with the European Convention on Human Rights (ECHR)

RIPA has been designed to ensure consistency with the ECHR and contains comprehensive safeguards regarding access to communications data. There are no proposals to remove any of these safeguards as and when other measures are taken to maintain the capability to access communications data in the future.

Use of mutual legal assistance conventions

Mutual legal assistance conventions are not an adequate alternative to the Government's proposed approach. Whilst the police take advantage of such arrangements to obtain communications data retained in other jurisdictions, their effectiveness relies on the national laws and procedures in the relevant jurisdiction, and also on whether that jurisdiction has the ability to respond. Moreover, mutual legal assistance is usually a slow process and could not meet the much shorter timeframes which apply during an ongoing investigation.

The UK Government regularly reviews mutual legal assistance procedures and aims to provide an efficient and effective service. Nevertheless, the UK can only respond to requests for communications data from other jurisdictions if such data is available, and if the requirements of our own legislation (including in terms of proportionality and necessity) are met.

D. CONCLUSION

The Home Office would like to thank all those who took the trouble to respond to this consultation.

The Government welcomes the recognition from a majority of respondents of the importance of communications data in protecting the public and that it is necessary to respond to rapidly changing technology in order to maintain this capability. It acknowledges that to improve confidence and trust in the use of communications data, and to demonstrate necessity and proportionality, it needs to continue to explain the importance of communications data, and the impact any loss of capability would have.

The Government will continue to develop the approach it proposed in the consultation document with a view to bringing forward the necessary legislation. In particular, it agrees with the significant view amongst respondents on the importance of safeguards and will ensure that the same strict safeguards that apply today will continue to minimise the potential for abuse and to ensure the safety and security of communications data under any new proposals. This view is strongly supported by public authorities that use communications data on behalf of the public.

The Government will also continue to work closely with communications service providers to ensure that any additional requirements will be feasible and reasonable, and to minimise, as far as possible, any impact on industry.

ANNEX A: GOVERNMENT ACTIVITY DURING CONSULTATION

Briefings

During the 12 weeks of the consultation briefings about communications data and the consultation were offered to a wide range of organisations and representatives, including:

- All Party Parliamentary Group on Privacy
- British Computer Society
- Confederation of British Industry (CBI)
- Parliamentarians
- Church of England
- Convention of Scottish Local Authorities
- Crown Agent (Scotland)
- Crown Prosecution Service
- Communications Service Providers
- Independent Reviewer of Terrorism Legislation, Lord Carlile of Berriew
- Information Commissioner
- Interfaith Network for the UK
- Internet Service Providers Association (ISPA)
- Law Enforcement Agencies
- Liberty
- NO2ID
- Privacy International
- Race for Opportunity
- Foundation for Information Policy Research
- Scottish Executive
- Security and Intelligence Agencies

Other consultations

During the period of this consultation, the Government carried out its consultation "Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice". That consultation closed in July but a copy of the consultation paper can be found at: http://security.homeoffice.gov.uk/ripa/about-ripa/ripa-consultations/.

The RIPA consultation was designed to assist the Government, amongst other things, to:

- review the public authorities able to authorise the use of communications data, covert surveillance in public places ('directed surveillance') and covert human intelligence sources, under RIPA;
- provide better guidance to ensure that the tests of necessity and proportionality are better understood and applied lawfully, consistently and with common sense;

- reduce bureaucracy by providing greater clarity on when authorisations are needed – and when they are not (in line with a recommendation in Sir Ronnie Flanagan's Review of Policing); and
- ensure that the constituency business of MPs is treated in the same way as other confidential material (following the report of Sir Christopher Rose into the bugging of conversations between Babar Ahmad and Sadiq Khan MP).

The Summary of Responses to that consultation, which more appropriately addresses some of the more general issues respondents to this consultation raised, is also published on the Home Office website.

ANNEX B: LIST OF RESPONDENTS

Responses were received from 167 members of the public and the following organisations:

Association of Chief Police Officers (ACPO)

AOL Europe

Association of Police Authorities

British Computer Society

British Medical Association

BSkyB

BT

Cable & Wireless

Child Exploitation and Online Protection Centre (CEOP)

Children's Charities Coalition on Internet Safety

Composite Software

Confederation of British Industry

Criminal Bar Association

Crown Prosecution Service

CTI Group UK

Detica

HP Enterprise Services

EXA Networks Ltd

Fife Fire and Rescue Service

Foundation for Information Policy Research/Open Rights Group

Gangmasters Licensing Authority

GCHQ

Hampshire County Council

Her Majesty's Revenue and Customs

Hutchison 3G UK Ltd

Information Commissioner's Office

Internet Service Providers Association (ISPA)

Islington Council

Justice

Kent Police

Liberty

London Internet Exchange Ltd (LINX)

Mayor of London

Metropolitan Police Service

Orange UK

Reviewer of Counter Terrorism Legislation (Lord Carlile of Berriew)

Police Federation of England and Wales

Police Service for Northern Ireland

Police Superintendents Association of England and Wales

Royal Mail

Royal Statistical Society

Security Service

Serious and Organised Crime Agency (SOCA)

Support after Murder and Manslaughter

Symantic Corporation

Telefónica O2 UK Ltd

Telecommunications UK Fraud Forum (TUFF)

Teradata

T-Mobile (UK) Ltd

Vodafone UK

Wiltshire Police

Yahoo! UK and Ireland

Yanaa Technologies

ANNEX C: BACKGROUND ON COMMUNICATIONS DATA

What is communications data?

Communications data is the information about a communication. It can show when a communication happened, where it came from and where it was going. But it does not include the content of that communication.

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

Why is communications data important?

Communications data plays a critical role in investigating and prosecuting serious crimes such as child sex abuse, kidnap, murder and drug related crime, as well as in public protection – such as locating missing persons. Communications data also prevents terrorist activities. It has, for example, played a significant role in all major Security Service operations since 2004. The police, the security and intelligence agencies and the emergency services all rely heavily on communications data. Without it they could not give the public the protection to which it is entitled.

How is communications data used?

Since the start of 2009, communications data has been essential in securing convictions in a number of major cases, including the Shakilus Townsend and Gooch Gang murder cases and in the Transatlantic Bomb Plot case. Yet this is just a small snapshot. Overall, communications data forms an important element of prosecution evidence in 95% of all serious crime cases. The ability to make use of communications data is therefore vital for our safety and security.

Access to communications data is regulated by RIPA, which places strict rules on when and by whom this data can be accessed. RIPA allows specified public authorities to ask for communications data related to an investigation but only when it is both necessary and proportionate to do so.

Why are particular challenges emerging now?

We now have access to many new forms of internet-based communications, such as social-networking sites, online role-playing games and instant messaging. Nearly 137 billion instant messages were sent in 2007 alone. There are now more mobile phones than people in the UK. Over 85 billion text messages where sent in the UK in 2008 - up from 63 billion in 2007. Whilst these new forms of communications undoubtedly bring many benefits, their effect on the way we can use communications data will be profound. They also present opportunities for criminals – who are quick to realise them. If we do not make changes to the way we collect and store communications data to accommodate technical change in the communications industry, the public will lose many of the protections to which they are reasonably entitled.

People are rightly concerned about the collection and storage of data regarding their use of telephones or the internet. The Government wants criminals and terrorists to be caught, but also wants privacy to be respected. That is why there must be – as there are now – safeguards strictly controlling how and by whom communications data can be obtained alongside independent oversight of its use. Whatever the technological changes, those safeguards must not be weakened – and indeed the Government will examine ways of strengthening them.

The Government has therefore been examining the full range of options for maintaining our capability to collect and use communications data in the face of this technological change. Getting the balance right between security and privacy has been central to this work.

Why is doing nothing not an option?

The consultation document made it clear that the Government believed 'doing nothing' in the face of challenges from rapidly changing technology was not an option. Doing nothing will undermine a crucial capability and result in diminished protection for the public. As some respondent noted, the Government would be failing in its duty if it did not address the challenges from rapidly changing technology.

ANNEX D: CASE STUDIES ON COMMUNICATIONS DATA

Case Study: a coastguard rescue

A walker who had become disorientated and lost in very poor visibility on the Isle Of Lewis, telephoned the Stornoway coastguards using his mobile phone. The caller reported that he was unsure of his position on the Moor but had managed to find shelter for himself and his dog. A rescue helicopter and four coastguard rescue teams were sent to the scene.

The use of telephone communications data was essential to finding this man, without which, coastguards would not have been able to approximate his location, and save his life.

(February 2009)

Case Study: 'Honey Trap' girl convicted of the murder of Shakilus Townsend

Shakilus Townsend, a teenager from South East London was lured to his death by Samantha Joseph, after becoming caught in a love triangle involving Joseph and Danny McClean, a gang member. Townsend was ambushed in a suburban cul-de-sac in South East London, by McClean and five other members of the Shine My Nine gang in July 2008. He was stabbed six times by two separate knives.

Communications data was used in this investigation to gather evidence of location points which could place the gang at the scene of the crime.

The gang members were convicted of murder in July 2009. Joseph has recently been sentenced to ten years and McClean to 15 years.

Case Study: Gooch Gang

The Gooch Gang wreaked havoc on the streets of Manchester by dealing drugs and using an arsenal of semi-automatic weapons. Colin Joyce, 29, and Lee Amos, 33, who led the gang were described by a senior police officer as 'psychopaths who shoot for fun'.

Communications data enabled officers to compile a hi-tech jigsaw of 80,000 mobile phone calls and texts to link the gang to their crimes. 11 convictions (including two life sentences for Joyce) were secured as a result on 8 April 2009. Shootings in Greater Manchester have also fallen by 92% in the last 14 months (as at July 2009) since the pair's arrest.

Case study: protecting vulnerable children

Julian Oliver, 36, came to the attention of law enforcement agencies, after an undercover policewoman in Australia, who had been posing as a young girl, was contacted by Oliver on a social networking site. He sent her sexually explicit messages, as well as a number of indecent images of children. Queensland police forwarded the information to the Child Exploitation and Online Protection Centre (CEOP), who were able to identify and locate Oliver. A search warrant of his house was issued and he was then arrested.

Over 1,600 images, and nearly 1,000 indecent movies of children were discovered. In July, Oliver was sentenced to two years in prison, and placed on the sex offenders register for life - preventing him from contacting or befriending anyone under the age of 16 for the rest of his life.

Case study: 'Drugs in Rugs' Gang gets 47 years

Over 16 kilos of heroin was concealed within straws which had been threaded through 25 rugs imported from Afghanistan. Analysis by the Forensic Science Service revealed the heroin was 75% pure.

HM Revenue & Customs officers at Birmingham airport discovered the drugs in January 2008 and alerted the Serious Organised Crime Agency. SOCA substituted the drugs rugs with dummies, replaced the original packaging, and began a surveillance operation when the gang came to collect them. After the gang's hire car was abandoned for the second time, SOCA investigators decided to switch from traditional surveillance and to focus instead on their other main lead – a single unregistered mobile phone number used by the gang to contact the courier company.

Analysis of phone data ultimately led to the identification of five men involved in the plot.

All five gang members pleaded guilty on the strength of the phone evidence. The four main players were sentenced at Birmingham Crown Court in June 2009 to between 10 years 8 months and 14 years 5 months for conspiracy to import Class A drugs.

ISBN 978-1-84987-097-9

Home Office
November 2009

HO_01332_G