ACCESS TO COMMUNICATIONS DATA

RESPECTING PRIVACY AND PROTECTING THE PUBLIC FROM CRIME

A consultation paper
March 2003

CONTENTS

FOREWORD BY THE HOME SECRETARY

1. It is not often that a piece of secondary legislation attracts the sort of attention that, last summer, engulfed the draft Order adding public authorities to the access to communications data provisions of the Regulation of Investigatory Powers Act 2000. In withdrawing the Order, dubbed a "Snoopers' Charter" by its critics, I admitted that we had got it wrong and said that we would have to think again and consult widely before returning to Parliament with any new Order.

2. On the face of it, legislation that sought to regulate access to communications data by public authorities, not extend it, should have been welcomed – or so we thought at the time. Two years had elapsed since the Act had been passed by Parliament and there was great pressure for the Government to clarify and regulate better the interchange taking place between public authorities and communications service providers around disclosure of communications data.

3. I take concerns about intrusion into privacy very seriously. I value my own privacy, and would be as concerned as anyone else if I thought that my mobile phone or other communications data could be easily available to an army of officials from public authorities.

4. In a democratic society, privacy is a right but not an absolute right. This is explicit in the European Convention on Human Rights, which permits compromise of an individual's freedom, but only in accordance with the law and where necessary to protect life or to prevent crime. Today, ensuring public safety and fighting crime – the most basic functions of the state – are shared by a wide range of public authorities. These are not "Big Brother" institutions acting against our individual liberty. Rather they are bodies working on our behalf to protect us from criminals, fraudsters and con artists or, in some cases, literally to save lives.

5. Nevertheless, I recognise that striking the right balance between respect for privacy and protecting the public is an issue for all of us, and it is important to get it right. Public authorities should be allowed access to communications data only when it is demonstrably both necessary and proportionate for this to happen. Applying these tests to the original Order has led us to conclude that it was too permissive and a more restrictive approach is necessary.

6. One option is to allow access to data only to a handful of additional public authorities: police bodies and the other emergency services. But it comes at a price in terms of reduced public protection and unsolved crime. Our preferred option is to reduce drastically the number of public authorities allowed to access the full range of communications data and to apply a range of additional restrictions and safeguards to the remainder. This would set in place, as a double lock, independent prior approval of access to communications data such as itemised telephone call records. There is a judgement to be made here; one that we are determined should be informed by wide public debate of the issues. I encourage you to join in that debate.

7. The concerns highlighted by the reaction to the withdrawn Order are only part of a much wider debate about the balance between privacy and protecting the public from crime. To succeed in allaying fears of a "Big Brother" approach by public authorities, Government needs to secure public confidence

that the boundary between privacy and protecting the public is set correctly. In a democracy, achieving that consensus, based on shared views and trust that the Government is acting on behalf of society not against it, requires that there is a open debate about the issues that concern all of us who care about our liberty and safety.

8. In addition to, and separate from the consultation on access to communications data, I would like your views on whether the time is fast approaching for that debate on how we strike the right balance between respecting privacy and giving public authorities access to the information they need in order to protect life and fight crime.

9. This consultation paper, which has been prepared with the help of an independent panel of experts, will I hope demonstrate that we have delivered on the promise I made to think again about proposals in the withdrawn Order. The issues raised around that Order are important and need to be debated if we are to achieve a consensus that commands public confidence. The consultation paper seeks to launch that debate.

DAVID BLUNKETT

SUMMARY

1. "Access to communications data – respecting privacy and protecting the public" is a consultation paper about how communications data is used by a range of public authorities to protect the public from crime. The paper describes their necessary and proportionate requirements for access to communications data and explores how those authorities might come within the regulatory framework provided by Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 (RIPA) for public authorities' access to communications data.

2. Within RIPA, there is a list of authorities that Parliament has agreed should have lawful access to communications data[1]. They are primarily law enforcement and intelligence agencies. This consultation paper does not seek to explore their need for access to communications data, which is widely understood and accepted. Rather it is concerned with additional public authorities that may be added to that list by Parliament.

3. We seek views that will help the Government to reframe the secondary legislation under RIPA governing access to communications data by additional public authorities in a way that addresses the concerns of the public, Parliament and interested organisations.

- In chapter two, we explain why public authorities need communications data, what data they need, how often they need it and, as far as possible, with what outcomes.

- In chapter three, we examine the criteria against which public authority access to communications data should be judged – based on the principles of necessity and proportionality – and describe safeguards for regulating that access. We explore options for imposing restrictions upon additional public authorities' access to data. We welcome views on the options and safeguard described.

- In chapter four, we explore some of the wider concerns about the balance to be struck by Government between respect for individual privacy and protection of the public from crime in the "Information Age". We welcome views on whether the time is right for a wider review of this issue.

4. The Government hopes the results of this consultation will deliver the widest possible consensus to enable the implementation of Chapter II of Part I of RIPA, extended to public authorities additional to those already agreed by Parliament. In advance of the consultation the Government's preferred approach is to restrict significantly the access of additional authorities – producing a radically different proposals to those laid before Parliament last summer. Nonetheless we welcome views on all the options explored in this paper.

1 They are: police forces (as defined in section 81(1) of RIPA); the National Criminal Intelligence Service; the National Crime Squad; HM Customs and Excise; the Inland Revenue; the Security Service; the Secret Intelligence Service; and the Government Communications Headquarters.

CHAPTER ONE **INTRODUCTION**

1. We are living in what has been described as an "Information Age". The rapid development of communications technology is transforming the way we live in a manner that would have been hard to imagine only a couple of decades ago. Most of us now take for granted access to instant communications, which we can use to send text, pictures or sound around the world in seconds. Some 80 per cent of households in the UK own at least one mobile phone[2]; 46 per cent of households have access to the Internet[3]. New technologies and applications are being developed all the time.

2. The growth in the availability and use of modern communications technology has been accompanied by an explosion in the amount of data that is created, processed and stored about us. Every time we use a mobile phone, send an e-mail or log onto the Internet, we add to the increasing volume of data about us.

3. The world is changing. This paper is about one aspect of that change – how public authorities tasked with prevention and detection of crime respond to the challenge of the use of communications technologies by suspects and criminals.

Communications data

4. The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content. In the case of a letter sent in the post, that data might include the names of the addressee and sender and the postmark showing where and when it was posted, all of which are on the outside of the envelope. It would not include the contents of the letter itself. Similarly, with calls from a mobile phone, communications data can comprise the telephone numbers involved, and the time and place of the call, but not what was said.

5. The box "What is communications data?" illustrates the variety of types of communications data. Some communications data can be more intrusive than other data: mobile phone location data pinpoints the place where a call is made, whereas subscriber data simply links names to phone numbers – information which can be obtained from commercially available software.

6. Communications data is generated by everyone, both law-abiding citizens going about their lives and criminals who use communications technologies to plan and organise their criminal activities and to seek to evade detection. And, just as criminals take advantage of such technologies to conduct their criminal activities, law enforcement agencies and other public authorities use the traces these technologies generate to help them to prevent and detect crime, and to protect the public. Matching a name to a telephone number, for example, can provide a vital link in the prevention and investigation of a crime. In an emergency, pinpointing the location from which a phone call was made can and does save lives.

7. Communications data can provide information unobtainable by other means, and can be instrumental in directing the course of an investigation. In the context of an investigation, historic itemised telephone call records will show that a call was made from A to B, when and for how long that call was made. Unless the parties to the call keep a record there will be not be one. Even where there are alternative ways of achieving the same outcome those will often be:

- less effective (ringing a phone number of a possible suspect to see who answers);
- more inefficient (physical surveillance is resource intensive and risks compromising the investigation); or
- more directly intrusive (placing a suspect under surveillance in public to investigate his contacts).

2 www.oftel.gov.uk/publications/research/2002/q10mobr1002.htm
3 www.statistics.gov.uk/CCI/nugget.asp?ID=8&Pos=1&ColRank=2&Rank=416

WHAT IS COMMUNICATIONS DATA?

Communications data does not include the contents of a communication. Within RIPA, communications data 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)).**

An indication of the sorts of information that might be included in each category is:

TRAFFIC DATA

- **information identifying the sender and recipient (including copy recipients) of a communication**
- **information identifying any location of a communication (such as mobile phone cell site location data)**
- **routing information identifying or selecting any apparatus (such as equipment, machinery or device, or any wire or cable) through which a communication is transmitted – for example, dynamic IP address allocation, web postings and e-mail headers (to the extent that content of the communication is not disclosed – the subject line of an e-mail is considered content)**
- **call detail records for specific calls (such as calling line identity)**
- **web browsing information (to the extent that only the host machine or domain name (web site name) is disclosed. For example, within a communication, data identifying www.homeoffice.gov.uk would be traffic data, whereas data identifying www.homeoffice.gov.uk/kbsearch?qt=ripa+traffic=data would be content.)**
- **information written on the outside of a postal item (such as a letter or parcel)**
- **online tracking of communications (including postal items)**
- **signalling information and dialling sequences that affects the routing of a communication (but not the delivery of information), in the investigation of "dial thru" fraud**

SERVICE USE INFORMATION

- **itemised telephone call records (numbers called)**
- **itemised connection records**
- **itemised timing and duration of service usage (calls and/or connections)**
- **information about the connection, disconnection and reconnection of services**
- **information about the provision and use of forwarding/redirection services (by postal and telecommunications service providers)**
- **information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services**
- **records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection**

SUBSCRIBER INFORMATION

- **subscriber information (known as 'subscriber checks' or 'reverse look ups'), such as "who is the subscriber of phone number 012 345 6789?", "who is the subscriber of e-mail account xyz@xyz.anyisp.co.uk?" or "who is the subscriber or who is entitled to post to web space www.xyz.anyisp.co.uk?"**
- **subscribers' account information, including payment method**
- **addresses for installation and billing**
- **abstract personal records provided by subscriber to service provider (such as demographic information or sign-up data (to the extent that password or personalised service access information is not disclosed))**

Public authorities and the need for regulation of access to communications data

8. Most of us accept that law enforcement agencies like the police should be able to use communications data to help bring criminals and those who threaten national security to justice. In a recent ICM survey, published in the Guardian[4], 72 per cent of those questioned agreed that giving up some privacy is necessary to fight terrorism and crime. When asked which organisations should have access to Internet and telephone records without first seeking authority from the courts, 65 per cent agreed that this should apply to the intelligence services, and 63 per cent the police.

9. Prevention and detection of crime and protection of public safety are not, however, the sole preserve of the law enforcement and intelligence agencies. A number of public authorities, with specialist functions and powers to investigate crime conferred on them by Parliament, today share that burden. The valuable work they do is not afforded the same level of public trust enjoyed by the police. In the same ICM survey, only half of those questioned were content for Government departments to access communications data without prior judicial approval. Trust in quangos (22 per cent) and local councils (19 per cent) was even lower. 21 per cent of people questioned believed no organisation should have such access.

10. The fact that the work done by some public authorities in fighting crime or ensuring public safety rarely makes the headlines nationally may be one reason why the withdrawn Order regulating access to communications data caused so much concern – as well as genuine surprise. Little of what they do now in accessing communications data is well known or much publicised, even though it has been done by well-established authorities for years – albeit on a much smaller scale than the police. They do so with no common standards or safeguards to ensure compliance with human rights legislation. The main benefit of the Regulation of Investigatory Powers Act 2000 (RIPA) is to provide a single regulatory regime for public authorities to access communications data compliant with human rights legislation, through explicit statutory requirements to take account of necessity and proportionality, statutory oversight of the exercise of powers and duties under the legislation and a statutory complaints mechanism about the exercise of those powers and duties.

The consultation paper

11. The Government hopes the results of this consultation will deliver the widest possible consensus to enable the implementation of Chapter II of Part I of RIPA, extended to public authorities additional to those agreed by Parliament. In advance of the consultation the Government's preferred approach is to restrict significantly the access of additional authorities – producing a radically different proposals to those laid before Parliament last summer. Nonetheless we welcome views on all the options explored in this paper.

12. This paper does not address issues around legislation[5] for the retention of communications data by communications service providers: a code of practice covering such retention on a voluntary basis is the subject of a separate consultation paper[6].

13. We welcome comments on any aspect of this consultation paper, whether on matters of general principle and policy or on the details of the proposals. All comments should be sent, by 3 June 2003, to:

Simon Watkin
Access to communications data consultation
Home Office
Room 732
50 Queen Anne's Gate
London
SW1H 9AT

Or comments can be e-mailed, by the same date, to:

commsdata@homeoffice.gsi.gov.uk

It will be assumed that respondents are content for their comments to be attributed to them and

4 www.icmresearch.co.uk/reviews/2002/guardian%2Dsuveillance%2Djuly%2D2002.htm Reported in The Guardian, 'Big Brother' supplement, p.3 (7 September 2002)
5 Part 11, Anti-terrorism, Crime and Security Act 2001
6 www.homeoffice.gov.uk/oicd/antiterrorism/consult.htm

made publicly available, unless the contrary is indicated. All responses may be included in statistical summaries of comments received.

14. This document is also available on the Internet:

www.homeoffice.gov.uk/ripa/part1/consult.htm

15. Any comments or complaints about the process of this consultation itself – as opposed to the specific issues addressed by this paper – should be made to:

Geraldine Lilley
Home Office Consultation Co-ordinator
7th Floor
Horseferry House
Dean Ryle Street
London
SW1P 2AW

Or by e-mail to:

geraldine.lilley@homeoffice.gsi.gov.uk

16. We would like to thank all those who have contributed to the consultation process so far. These includes our panel of independent experts (see annex A), who reviewed the material we collated and commented on drafts of this paper; colleagues from other Government departments (particularly the Lord Chancellor's Department); industry and trades union representatives; and others who submitted comments in writing and in discussions online.

CHAPTER TWO PUBLIC AUTHORITIES AND ACCESS TO COMMUNICATIONS DATA

1. The purpose of the draft Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002[7] laid before Parliament in June 2002 was to regulate access to communications data, not to extend it. Much of the criticism of the Order misunderstood what data public authorities would be allowed to access. In some quarters it was presented as a "Snoopers' Charter", allowing vast numbers of officials from public authorities to snoop on the content of e-mails and other types of communication. In fact, the Order had nothing to do with the content of communications, electronic or otherwise.

2. Nonetheless, the criticism of the Order struck a chord. Partly this reflected genuine and widespread surprise at the large number of public authorities listed on the Order. The lack of any public consultation exercise undoubtedly contributed to this, as little was known about the reasons why public authorities need access to communications data – and even less about how they currently obtain it.

3. The Government also failed to explain that the Order would have been qualified by a second Order, the Regulation of Investigatory Powers (Communications Data: Prescription of Offices, Ranks and Positions) Order 2002[8]. This would have made clear which individuals in which specific parts of the public authorities were to be authorised to access communications data, and for what statutory purposes.[9]

4. As an example, the initial Order listed the Department for Transport, Local Government and the Regions (DTLR).[10] The second Order would have qualified this to mean the Maritime and Coastguard Agency, and within the Agency, only two people would normally have access to communications data, rising to a maximum of eleven people in a search and rescue emergency and only for the specific purposes of preventing and detecting crimes investigated by the Agency, and preventing death or injury in an emergency.

5. Many of the additional public authorities that were within the scope of the Order laid before Parliament in June, or which could be included in any future Order, already have access to communications data using statutory powers to require disclosure of information[11]. But public awareness of this and the reasons for it is low. Adding to the RIPA regime public authorities that already have statutory powers that can be used to access communications data would not extend or restrict their ability to obtain that data. It would, however, ensure that such access was regulated by RIPA procedures and safeguards, under the oversight of the Interception of Communications Commissioner. Other, new, public authorities do not currently access communications data but can show a need to do so.

6. The extent to which the additional public authorities currently access communications data should be seen in context. The police service, together with the other authorities listed in RIPA, make approximately half a million requests for communications data annually.[12] In contrast – excluding the Scottish Drug Enforcement Agency's 55,000 requests a year – the total number of requests by the additional public authorities is approximately 23,000 a year, or around 4 per cent of all requests[13]. We do not anticipate implementation of Chapter II of Part I of RIPA leading to a dramatic increase in the number of requests[14] for communications data, or a

7 www.homeoffice.gov.uk/ripa/part1/orders.htm
8 www.homeoffice.gov.uk/ripa/part1/orders.htm
9 Consideration is being given to whether one composite Order could be laid instead. If not, the Government would intend to publish any revised Orders simultaneously, in order to minimise misunderstanding of the scope of the first Order.
10 The DTLR no longer exists. The Department for Transport is responsible now for the Maritime and Coastguard Agency.
11 Annex B addresses human rights law, the Data Protection Act 1998, statutory means of accessing communications data, and RIPA
12 In the absence of a single regulatory regime for access to communications data by public authorities, there is no requirement to record the extent to which requests for data are made. The figures given in this paper are approximate. The RIPA code of practice will require precise record-keeping.
13 Figures are not available for all authorities, in particular locally managed fire authorities and emergency ambulance services

change in the profile of type of data being accessed. Approximately 90 per cent of all requests for communications data are for subscriber information.

7. In this chapter, we explain why a wide range of public authorities need access to communications data to investigate crime and to ensure public safety. We see such openness as an important part of building public trust in their work. This covers:

- Who accesses communications data?
- What types of communications data?
- On what scale?
- And with what results?

8. Detailed information[15] – significantly more than has previously been publicly available – about public authorities' need for communications data is online at **www.homeoffice.gov.uk/ripa/part1/pas.htm.**

In addition to those authorities on the original Order, this information covers ambulance services, the Serious Fraud Office, the Gaming Board for Great Britain and the Charity Commission, all of which could be included in any new Order to be laid before Parliament.

Additional public authorities

9. The additional public authorities seeking access to communications data under RIPA fall into three categories:

- police bodies;
- emergency services; and
- agencies or public authorities with functions to investigate specific and often specialised offences or conduct.

Police bodies

10. The Order laid in early summer included two police bodies: the Scottish Drug Enforcement Agency (SDEA) and the United Kingdom Atomic Energy Authority Constabulary (UKAEAC).

11. Formally established in April 2001, the SDEA incorporates what were the Scottish Crime Squad, the Scottish Criminal Intelligence Office and the Scottish Technical Support Unit. It has been compared in remit to the National Crime Squad, which covers England and Wales and is listed in RIPA[16]. The SDEA co-ordinates the intelligence and operational elements of drug enforcement and the investigation of drug trafficking and serious and organised crime in Scotland. It made over 55,000 requests for communications data of all types in 2001-02. During this period, communications data played a vital role in the seizure of more than 200 kilograms of class A drugs and 1000 kilograms of class B drugs, the arrest of 185 criminals involved in drug trafficking and other forms of serious and organised crime, the disruption of 73 criminal networks and the identification of £1,263,544 in realisable assets.

AN SDEA INVESTIGATION

The SDEA operates on the front line of the war against drugs in Scotland. One drug trafficking case involved ten suspects and drugs with a street value of over £500,000 over a period of two years. Subscriber, call records and traffic data were all used in the intelligence operation to identify drug couriers and safe houses. The principal defendant was sentenced to seven years imprisonment, and his main associates to five and three years respectively. Criminal assets to the value of £322,579 were identified for restraint.

12. UKAEAC is the third largest non-Home Office police force in the UK, after the Ministry of Defence Police and the British Transport Police. It protects designated civil nuclear sites and special nuclear materials in storage and transit. On the rare occasions when intruders may breach perimeter security controls and are arrested within nuclear establishments, it may be necessary to check telephone numbers in mobile phones, hand held computers, or paper documents for terrorist or criminal links. UKAEAC is also

14 Under RIPA access to data is made by way of a Notice or Authorisation (see Annex B, paragraph 28)
15 This information has been collated by the Home Office from data provided by the public authorities or their representative bodies
16 Section 25(1)

responsible for preventing and detecting routine crime within its jurisdiction. So, for example, in one case, analysis of itemised telephone call records and identification of locations from subscriber checks led to the recovery of a large amount of stolen property, valued at £75,000.

Emergency services

13. Fire authorities and the Maritime and Coastguard Agency of the Department for Transport use communications data for three reasons – locating callers in an emergency, tracing hoax calls, and conducting investigations – while the emergency ambulance services of Ambulance Service NHS Trusts[17] need communications data for the first two reasons only:

- Call location data is needed to facilitate a fast response in emergency situations where the caller is unable to give his position (either because he does not know or because he is incapacitated). Communications data is thus used to prevent death and serious injury. One caller rescued from a fire commented 'I think it was remarkable how you managed to trace that call and I know if you had not been able to do [so] I would not be here today.' In 2001, the Maritime and Coastguard Agency saved 12 lives through use of communications data.

- Secondly, emergency services receive a significant number of hoax phone calls each year, as has been highlighted during the fire service dispute. This may even involve ambush – for example, attacking fire engines using fireworks and bricks. The use of communications data is crucial to identifying and successfully prosecuting malicious callers. Fire authorities in England and Wales received 63,837 hoax phone calls in 2000; figures for Scotland and Northern Ireland were 7,976 and 5,879 respectively. The Maritime and Coastguard Agency received approximately 200 hoax calls in 2001. The cost to it of responding to a malicious call can be well over £100,000. The police usually tackle hoax calls made to the ambulance services, but where the police do not investigate, the relevant emergency ambulance service will pursue the matter. Statistics on the number of hoax calls made to ambulance services are not available.

- Lastly, fire authorities conduct investigations into the cause of fires and the Maritime and Coastguard Agency undertake investigations to prevent and detect crime relating to maritime safety and pollution. In 2001, inspections revealed approximately 90 potentially significant breaches – defined as potential or actual serious damage to a ship or equipment or the environment, or potential or actual serious injury or loss of life. The inspections resulted in 16 prosecutions, with 10 cases resulting in either the cautioning of the offender(s) or a notification of concern being issued to the persons involved.

14. The need for the emergency services to be able to access communications data, including mobile phone location data, has not been considered contentious. Although European Directives on communications and data protection provide that communications operators may release information to the emergency services in an emergency or to trace malicious calls, inclusion of the emergency services within the RIPA regime will provide a regulated framework within which they can use that data.

15. Frequency of access to communications data for fire authorities and emergency ambulance services is not known; total estimated use for the Maritime and Coastguard Agency is less than 300 annually (of which approximately 35 would be for enforcing maritime safety and pollution legislation).

Agencies or public authorities with functions to investigate specific and often specialised offences or conduct

16. The majority of public authorities to be covered by the Order under Chapter II of Part I of RIPA investigate specialised offences. The work they do and the need they have for access to communications data is as varied as the offences they investigate, but those crimes all have an impact on people's lives and the communities they live in.

17. Several public authorities dealing financial crime use communications data.

17 In Scotland, the Scottish Ambulance Service Board; in Wales, the Welsh Ambulance Services NHS Trust; in Northern Ireland, the Northern Ireland Ambulance Service Trust

18. The Financial Services Authority has a statutory objective to reduce financial crime and investigates and prosecutes a range of offences relating to financial services and markets, including insider dealing. On conviction they can carry sentences of up to seven years imprisonment. The offences are costly to consumers and potentially damage the integrity of UK financial markets. The Financial Services Authority is increasingly involved in detecting such criminal activity conducted by telephone or the Internet. Communications data can be critical in proving whether or not offences have occurred in those contexts. It is a criminal offence to carry out financial business without the requisite authorisation from the Financial Services Authority. In the year to November 2002, telephone and Internet subscriber data was obtained in the course of 66 enquiries into the possible conduct of unauthorised business. In such inquiries, subscriber data can be crucial in determining whether the business has taken place within the UK and therefore within the Financial Services Authority's jurisdiction. These are matters that have not always led to formal investigations or proceedings, but on the basis of a representative sample of these cases, the Financial Services Authority estimate that in approximately 20 per cent, unauthorised business has been discovered and stopped. The Financial Services Authority currently uses communications data approximately 100 times per annum, but this figure is expected rise.

19. The Office of Fair Trading (OFT) is the principal competition authority in the UK, responsible for safeguarding competition and protecting consumers. Access to communications data is only sought by the Cartel Investigation Branch within OFT, which needs to access communications data to investigate cartels (prosecution will be by the Serious Fraud Office): the Enterprise Act 2002 made dishonest participation in a cartel a criminal offence punishable by five years imprisonment.

TACKLING INSIDER DEALING

Insider dealing includes the illegal practice of trading in stocks and shares to one's own advantage through having access to confidential inside information that would be likely to affect the value of those stocks and shares. Communications data showing contact at critical times between individuals suspected of insider dealing is frequently a key investigative tool and often forms an important part of the evidence in insider dealing cases.

In one investigation of insider trading by the Legal Services Directorate of the DTI, almost the entire case rested on the date and time of telephone calls made between the various defendants. Telephone records were obtained from business and home telephone numbers with the Brokerage firm providing details of incoming and outgoing calls to clients. One defendant received a three-month prison sentence. Another received a fine.

20. Three units within the Department of Trade and Industry (DTI) have applied for access to communications data under RIPA. Two of them deal (in different ways) with corporate and financial wrongdoing and crime:

- The Companies Investigations Branch carries out fact-finding investigations under (among others) the Companies Acts and the Financial Services and Markets Act 2000, to establish whether particular offences have been committed or whether criminal conduct may be involved.

- The Legal Services Directorate[18] conducts criminal investigations and prosecutions in relation to offences under (among others) insolvency, insider dealing and companies legislation.

FRAUDULENT TRADING

The Legal Services Directorate of the DTI investigated a case of fraudulent trading in which the trader subscribed to telephone numbers under a variety of names but re-routed the calls to a single telephone. Analysis of subscriber details enabled the investigator to prove links between the subscriber, the calls and the fraudulent trader. The trader was sentenced to four and a half years imprisonment.

18 Specifically Directorate D of the Legal Services Group

21. As with the other bodies operating in the area of financial crime, being able to gain access to communications data is an important investigative tool for these two units of the DTI. Together, they require access to communications data approximately 200 times per year.

22. In 2001-02 the Companies Investigations Branch initiated 153 investigations, of which 118 involved allegations of fraudulent trading. Communications data plays a part in approximately five per cent of all the investigations by the Companies Investigations Branch which involve allegations of criminal conduct. The Legal Services Directorate currently has over one thousand criminal investigations ongoing and whilst accurate details of the number of cases in which communications data feature are not available, it is estimated that between five and ten per cent of successful prosecutions rely to varying degrees on communications data.

23. The third DTI body that has applied for access to communications data under RIPA is the Radiocommunications Agency, which is responsible for managing the civil radio spectrum by enforcing the Wireless Telegraphy Act 1949. It uses communications data in, for example, the investigation of pirate radio stations. Illegal use of the civil radio spectrum, as well as having an economic impact on legitimate business, can affect public safety by, amongst other things, interfering with aircraft landing systems. Parliament is currently being asked to make subject to arrest those involved in pirate radio, hoax radio calls to emergency services, and deliberately interfering with radio communications[19]. The Radiocommunications Agency presently seeks access to communications data approximately 400 times per year.

24. The Serious Fraud Office investigates and prosecutes cases of serious or complex fraud in England, Wales and Northern Ireland, in order both to reduce fraud and maintain confidence in business and financial institutions. As with many of the other bodies investigating financial crime,

PIRATE RADIO STATIONS

Communications data is routinely used by the Radiocommunications Agency to prosecute those running pirate radio stations. In one case, searching a pirate radio studio led to an individual's business card being found. On that card were two telephone numbers: a land line and a mobile. Amongst other items seized from the studio was a mobile telephone and advertising material for the pirate station. The mobile number on the business card was found in the missed numbers record of the mobile telephone and appeared on the advertising material. A subscriber trace of the telephone numbers on the business card provided the home and business addresses of the individual. A search warrant for the business premises was obtained. The search resulted in the discovery of material relating to the operation of the pirate radio station, and the conviction of an individual for participating in the management of that station. The sentence on conviction was a 120-hour Community Punishment Order and £500 costs; in addition, the Radiocommunications Agency obtained forfeiture of all the equipment, etc it had seized.

Subscriber data has also been used successfully to support prosecutions of suppliers of radio equipment that conflicts with UK radio spectrum use and is therefore likely to cause harmful interference to authorised radio systems such as airport and aircraft transmissions.

	2001	2002
Pirate radio stations investigated	248	209
Suppliers of illegal radio equipment investigated	18	24
Requests for communications data made	316	368
Persons prosecuted for their involvement with pirate radio stations	20	49
Persons prosecuted for selling illegal radio equipment	0	3
Prosecutions where communications data formed part of the case	3	7

There are 26 prosecutions pending in which communications data forms part of the case. The increased prosecutions and use of communications data can be attributed to strategy implemented a year ago to target more resources at identifying those responsible for the operation of pirate radio stations.

19 In the Communications Bill currently before Parliament

communications data may be used in evidence during trial to show connections between individuals in insider trading circumstances. It may also be used to identify money flows, support evidence of conspiracy or to give true identity to aliases. The Serious Fraud Office currently uses communications data between 36 and 48 times per annum.

25. The Immigration Service (Enforcement Directorate and Intelligence Directorate) of the Home Office has the lead role in investigating organised immigration crime including the smuggling of people and illegal working cartels, asylum abuse, fraud, deception and other immigration related offences. Immigration Officers can enter, search, seize and arrest under powers linked to criminal offences within immigration legislation. Communications data can help identify those involved in offences such as people trafficking, and any links between different persons or organisations. The Immigration Service anticipates having around 100 requirements for communications data per month.

TACKLING PEOPLE SMUGGLING

As part of an investigation into people smuggling, information was received that an individual employed by a public company was involved in assisting illegal entry into the UK. The personal telephone number of the suspect individual was provided. Subscriber checks confirmed that he was the owner of the telephone. Through itemised telephone call records and analysis it was confirmed that he was in regular contact with other employees working in the same company. The pattern of calls matched the movement of illegal entrants. This provided the intelligence to support a pro-active investigation that was, in this case, undertaken by the police and culminated in the arrest and conviction in October 2002 of three persons involved in this case of people smuggling. All received substantial custodial sentences.

26. The Health and Safety Executive (HSE) enforces health and safety requirements in sectors such as railways, construction, agriculture, manufacturing, and in the chemicals, offshore and nuclear industries. HSE investigates possible offences under health and safety legislation which may involve the creation of serious risks to people's health and safety, or actual serious injury, occupational ill-health, or deaths. Health and safety incidents include explosion or poisoning from faulty domestic gas installation, railway incidents, inadequately protected workers falling from heights at construction sites, or exposure to asbestos and the consequent long term threat of terminal lung damage and cancer.

27. In England and Wales, the HSE also prosecutes the offences it investigates. In Scotland, it advises the Procurator Fiscal (a local coroner and public prosecutor) on the prosecution of health and safety matters. Breaches of health and safety legislation are criminal offences, and the Government plans to make nearly all such offences imprisonable, instead of the present few, to reflect their potential seriousness.

COMMUNICATIONS DATA AND RAILWAY ACCIDENTS

When investigating incidents on the railways – whether train crashes or accidents involving track workers – it can be important to ascertain whether the mobile phone(s) of the individual(s) involved were in use at the time of the incident. Communications data provides evidence of this, and thus can aid significantly the Health and Safety Executive's investigation, help establish underlying causes of an accident to prevent future injuries or deaths, and assist in the prosecution of any serious offence committed.

28. HSE obtains communications data in order to trace and investigate individuals or businesses whose work activities may be putting people at risk of serious harm. Communications data might also be sought where other means of tracing an undertaking would be too slow to allow possible serious risk to be averted. Communications data is also sometimes needed because mobile phone use may be among the causes of an incident; the timing of mobile phone use may also reveal important information about what was being done to reduce risks before and after an incident. HSE only seeks access to subscriber information and information from itemised telephone call records under RIPA.

29. In 2000-01, 33 people were killed and 301 suffered major injury by gas explosion or carbon monoxide poisoning because of faulty domestic

gas installations. In addition, 5,880 instances of dangerous gas fittings and were reported to HSE. Full investigation of the most serious events led to 60 prosecutions and the issuing of about 220 enforcement notices, the vast majority against installers and landlords in breach of their statutory duties to ensure gas safety for members of the public. In some cases, the only information available to the investigating inspector is a forename and telephone number. Obtaining communications data has enabled prohibition notices to be issued and prosecutions to be brought, preventing further possible harm. Indeed, non-registered gas installers under investigation can go to some lengths to prevent HSE getting their address, making communications data vital. Some investigations have been terminated because disclosure of this information has been refused, leaving incompetent installers to continue working unchecked.

TRADING STANDARDS FUNCTIONS OF LOCAL AUTHORITIES

Northampton trading standards officers investigated a rogue plumber and gas fitter who traded under false names and used different telephone numbers to avoid detection. Consumers were defrauded and their safety was put at risk as he was a non-CORGI [Council for Registered Gas Installers, the national watchdog for gas safety in the UK] registered plumber 'servicing' gas appliances. Subscriber phone details were required to successfully trace his activities. He was sentenced to 9 months in prison in November 2000.

Brighton and Hove Trading Standards used communications data to investigate a 'mock auction' shop run by rogue traders. The operation dishonestly sold shoddy goods at high prices: takings were approximately £75,000 in five weeks. Communications data was crucial to the success of the injunctive proceedings as it enabled them to prove a chain of supply and pattern of activity by the defendants.

Subscriber information and itemised telephone call records were crucial in enabling Bracknell Forest Trading Standards to gain the conviction of four defendants to four years imprisonment each for their involvement in counterfeiting £20 million worth of computer software.

30. A few cases per year arise in other sectors. In one case, second-hand tanks for liquids were being sold on without asbestos being removed properly, putting buyers and public at risk of harm. HSE obtained telephone records that allowed inspectors to track down the supplier quickly, thus minimising the risks to which people were exposed.

31. The addition of local authorities to Chapter II of Part I of RIPA attracted significant attention over the summer. But local authorities have a number of statutory enforcement functions, many of which are their sole responsibility. Access to communications data is required for only certain of those, including:

- Trading standards investigations in relation to consumer protection legislation – for example, car fraud, counterfeit goods, consumer scams and rogue traders.
- Environmental health investigations in relation to public health and food safety legislation.
- Housing benefit and planning investigations, for example in relation to benefit fraud, anti-social behaviour orders, landlord-tenant harassment (itemised telephone call records could be used to ascertain the extent of contact between landlord and tenant), preservation orders, and improper constructions on premises.

32. The ability to access and disclose communications data is essential to enable local authorities to effectively carry out investigations in these areas, which can involve fraud, theft and other serious criminal offences. Local authorities protect their local citizens, which include vulnerable groups such as the elderly, young, and disadvantaged sectors of the community.

33. The majority of local authority requirements for communications data relate to trading standards investigations. Figures are incomplete and seem to fluctuate, but an extrapolation of data available for 2000 and 2001 suggests an average of about 17,000 requests for communications data (the vast majority of which were for subscriber details) are made by local authorities per year. The number of requests for communications data is large in volume, but that is not altogether surprising, since local authorities enforce a wide range of legislation.

34. Local authority representatives and the Government have looked again at the way in which local authorities were defined on the Order laid last summer – which potentially enabled parish and community councils to access communication data. Any revised Order will exclude parish and community councils from the definition of local authorities able to access such data.

35. The Trading Standards Service of the Department of Enterprise, Trade and Investment for Northern Ireland is responsible for the investigation of trading standards matters in Northern Ireland. It estimates requiring communications data about 100 times annually.

36. The Environment Agency and the Scottish Environment Protection Agency both investigate and prosecute environmental crime – under environmental protection, fisheries, and pollution legislation. The Environment Agency investigates, for example, unregistered waste disposal operators. Much of the waste taken on by these groups is fly-tipped. Fly-tipping on agricultural land alone costs society £60 million a year, as well as damaging the local environment and potentially harming those who live there. This kind of crime is attractive to criminals because it is a low-risk, high-profit activity. The Environment Agency requested communications data 469 times in 2001-02. The vast majority of requests that the Environment Agency makes are subscriber checks; it also makes a small number of requests for itemised telephone call records. The Scottish Environment Protection Agency has no history of using communications data, but is moving into the fields of work undertaken by the Environment Agency, and so anticipates similar needs to that body.

37. Three bodies within the Department for Environment, Food and Rural Affairs (DEFRA) have requested access to communications data under RIPA.

38. The Investigation Branch and the Centre for Environment, Fisheries and Aquaculture Science enforce legislation relating to animal health and welfare (e.g. foot and mouth disease), environmental issues, veterinary medicines and pesticides. The Investigation Branch provides a criminal investigation service to DEFRA, its agencies, devolved administrations and the Forestry Commission. Communications data can be used in many different situations, for example:

- Identifying individuals undertaking organised importation and sale of unauthorised veterinary medicines. Dealers exploit price differentials between Great Britain and other countries and prescription-only medicines are administered to animals without the supervision of a vet. These activities not only compromise animal welfare but the uncontrolled use of antibiotics or other products in food animals represents a threat to human health.
- Investigating the black market in undeclared catch (fish caught above official quotas). The market relies on telephone contacts to make sales; communications data has a role to play in investigating such activity.

39. The third DEFRA body is the Counter Fraud and Compliance Unit of the Rural Payments Agency. The Rural Payments Agency is responsible for the administration and payment of funds, such as the EU Common Agricultural Policy. It has a legal duty to protect taxpayers' money distributed through the EU and deter and tackle fraud (similar to Inland Revenue and Customs and Excise in dealing with Exchequer monies). The Counter Fraud and Compliance Unit provides a criminal investigation and enforcement service in respect of the Rural Payment Agency's responsibilities. The matters investigated vary in size and value but can involve widespread abuse totalling in excess of a million pounds. The Public Accounts Committee of the House of Commons has called for the Rural Payments Agency to do more to tackle such fraud. The Counter Fraud and Compliance Unit might use communications data when:

- Investigating the black market in undeclared milk (milk produced and sold outside the quota regulations). As with the markets investigated by other DEFRA bodies, it relies on telephone contacts to arrange collection and delivery between unregistered parties, so communications data is a useful investigative tool.

40. The three DEFRA bodies use communications data infrequently: they anticipate approximately 30 occasions per annum between them. They do not need traffic data.

41. Established in April 2000 in response to BSE ("mad cow disease") and other food scares, the Food Standards Agency protects the public and investigates crime within its specialist field. Its

role is to protect public health from risks that may arise in connection with consumption of food, to protect the interests of consumers in relation to food, and to enforce food safety standards. The Agency is the enforcement authority in respect of around 1,600 licensed premises in Great Britain producing meat for sale for human consumption. Communications data proves useful to investigations in identifying, for example, suppliers of illegally produced meat or intermediaries to whom it is supplied. However, the Agency anticipates needing subscriber data or itemised telephone call records on only one or two occasions per year.

SELLING MEAT UNFIT FOR HUMAN CONSUMPTION

During a joint investigation with the police, a Food Standards Agency search of food premises revealed a notebook containing a telephone number which, by means of subscriber information, was traced to an alleged supplier of illegally produced fresh meat that was unfit for sale for human consumption.

42. There are two bodies coming under the umbrella of the Department of Health that have applied for access to communications data through RIPA:

- the Medicines Control Agency, and
- the Medical Devices Agency.[20]

UNSAFE MEDICINES

Cases involving the illegal sale and supply of Gamma-Hydroxy Butyrate (GHB) are regularly reported to the Medicines Control Agency. GHB is used as a "date rape" drug and as a recreational drug on the club scene. Adverse reactions include induced coma, slowed heart rate and death. In one case, the Medicines Control Agency was unable to trace the owner of a mobile phone who was ordering the raw material through a manufacturer and the case had to be closed, thus allowing the source to continue operating. Penalties for offences under the Medicines Act are an unlimited fine and a two-year term of imprisonment.

43. The Medicines Control Agency has a statutory duty to protect public health by ensuring the safety, quality and efficacy of medicines on the UK market. Unlicensed medicinal products pose potentially significant health risks and can be fatal; the Medicines Control Agency prevents, detects and prosecutes crime in this area. For example, certain unlicensed and untested "traditional Chinese medicines" have been found to contain cancer-causing substances. Another illegal activity involving medicines is the supply of prescription-only medicines without a prescription – including Viagra and certain slimming drugs. Such drugs can be dangerous if not taken under the strict supervision of a health professional. The advertising and sale of these drugs is often conducted via a PO Box number or by telephone and, increasingly, the Internet and consequently communications data can prove crucial to a successful investigation and preventing a potentially unsafe product from reaching its intended customers.

44. The Medical Devices Agency investigates offences under consumer protection legislation and EU directives in respect of medical devices on the UK market. The circumstances in which it might need communications data include investigating a manufacturer of an unsafe medical device selling its product by listing a contact number on the Internet or product literature. Identifying the owner of the telephone number may be the only way to trace the provider in order

DANGEROUS MEDICAL DEVICES

Attempts to remove non-compliant medical devices from the UK market have been frustrated when companies use PO box numbers. In one case, an overseas manufactured 'miracle' bracelet (claimed to alleviate arthritis, anxiety, varicose veins, tachycardia, kidney complaints and respiratory problems) could not be removed from the market even though it did not meet the statutory requirements and posed a risk to public health. This was because a UK distributor presence could not be identified without access to communications data. If the case had reached prosecution stage, the UK supplier would have faced a maximum fine of £5000 or a six-month prison sentence.

20 In April 2003, the Medical Devices Agency and the Medical Control Agency are to merge: the new body will perform the functions of both existing agencies.

to remove unsafe products from the market or ensure compliance with relevant legislation, and to identify consumers of unsafe products.

45. Both the Medical Devices Agency and the Medicines Control Agency expect to use communications data on approximately 20 occasions per annum. They do not have any existing powers to access communications data, but their enforcement functions mean that they have powers of entry, search and seizure.

46. Also needing access to communications data are the NHS Counter Fraud and Security Management Service (NHS CFSMS)[21], and its equivalents in Scotland (NHSScotland Counter Fraud Services[22] of the Common Services Agency for the Scottish Health Service) and Northern Ireland (the Counter Fraud Unit of the Northern Ireland Central Services Agency for Health and Social Services).

47. These three bodies tackle fraud and corruption within the NHS (NHS CFSMS covering NHS fraud and corruption in Wales as well as England). NHS CFSMS also has the remit for tackling fraud and corruption within the Department of Health and its agencies. Additionally it deals with security management within the NHS in England (though not Wales): its Scottish and Northern Irish counterparts do not perform this function within their own country.

HEALTH FRAUD

An NHS Estates Manager was suspected of corruptly awarding contracts to a building firm in return for gifts and favours. Although the manager was eventually disciplined for not following normal contract and tendering procedure, no action could be taken against the contractor involved, as the investigation was unable to prove that there was any abnormal or unusual contact between the two parties. Subscriber information and itemised telephone call records would have enabled investigators to establish home telephone numbers (both were ex-directory) and whether there was any "out of hours" contact between the two, but the data holder declined to disclose the data under the Data Protection Act 1998. Losses were difficult to quantify as the investigation could not be successfully completed, but one audit estimated that the Trust concerned was probably paying around £150,000 per year over and above what it should have been. If the offence had been proved, the maximum sentence would have been seven years imprisonment.

48. NHS CFSMS anticipates using communications data approximately 100 times per annum in England and Wales; its Scottish and Northern Irish counterparts anticipate using such data less than 10 times per annum each. Subscriber and telephone call records information, for example, can be used in fraud and criminal investigations to investigate a wide range of fraud perpetrated against the NHS, such as false claims for services not provided to patients by NHS contractors.

49. The Department for Work and Pensions (DWP) was listed on the original Order so that the Counter Fraud Investigation Division (Operations) and the Counter Fraud Investigation Service could access communications data under RIPA. This body investigates allegations of fraud against social security benefit systems and prosecutes where appropriate. This type of fraud costs the taxpayer between £2 billion and £4 billion each year. Communications data can aid investigations of significant, organised benefit fraud, by assisting in tracking movements of organised gangs involved in major counterfeiting and multiple identity attacks on the benefit system. Communications data can also be used to help investigations of smaller scale fraud: undeclared working or living together. DWP counter fraud investigators require communications data approximately 2,500 times per annum.

50. The Information Commissioner investigates and prosecutes offences under the Data Protection Act 1998 (DPA). These are commonly concerned with the violation of individuals' privacy through the unlawful obtaining and selling of personal information held by organisations such as banks, health centres, Inland Revenue and the DVLA. 95 per cent of the time, this data is obtained using a

21 NHS CFSMS was created on 1 January 2003 as a Special Health Authority, under the NHS Act 1977, and is a public authority in its own right. When the original RIPA Chapter II Order was laid, it was NHS Counter Fraud Services, part of the Department of Health.

22 Before 28 February 2003, this was known as the Fraud Investigation Unit

telephone as this affords anonymity to the perpetrator. In 2001-02, the activities of the Information Commissioner's Investigations Department comprised:

- 106 cases submitted for consideration of prosecution
- 66 cases brought to court
- 3 search warrants obtained

51. Communications data was used in the majority of cases and search warrants. It is an important element in proving that an offence has been committed. In the twelve months to September 2002, 88 requests for communications data were made (52 for subscriber checks, 36 for itemised telephone call records).

PROTECTING PERSONAL DATA
In one case, a firm repeatedly contacted the Benefits Agency in order to obtain unlawfully personal data. Subscriber information identified the company concerned; itemised telephone call records illustrated the scale on which the company was contacting that body.

In another case, a company contacted a health authority attempting to obtain unlawfully personal data. Subscriber and itemised telephone call records were similarly used to investigate that conduct.

52. The Information Commissioner currently accesses data as a prosecuting authority for offences under the DPA. Section 58 states that 'No enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing the Commissioner or the Tribunal with any information necessary for the discharge of their functions under this Act.'

53. There are two bodies working in the field of postal services that use communications data in investigations.

54. The Royal Mail Group plc[23] is a Universal Service Provider within the meaning of the Postal Services Act 2000. Its security and investigation services investigate and prosecute offences[24] committed against Royal Mail Group by both employees and third parties. This includes theft of mail by postal workers, theft of money and benefits payments by Post Office staff, burglaries at Post Offices, robberies from postal workers, obtaining postal services by deception and malicious communications. Royal Mail Group made applications for communications data 361 times in 2000-01, and 418 times the following year. It uses subscriber and itemised telephone call records.

ROYAL MAIL GROUP PLC
In one case, corruption was suspected between Royal Mail Group Senior Managers and an external company in awarding a £2.7 million contract. Communications data was used as evidence in the case. Another investigation concerned the embezzlement of funds by a Senior Manager within the organisation. Communications data was used to establish links with external parties and to trace the location of missing funds. £1.6 million in losses were confirmed and subsequently recovered; and two arrests made.

55. The Postal Services Commission (Postcomm) – the independent regulator for the postal service within the UK, responsible for protecting the interests of the postal industry and its users, and for licensing operators – is the lead body for investigating infringements of the Postal Services Act 2000. These include delivering letters without a licence and interfering with mail while in the course of delivery. The Postal Services Commission was established in November 2000 and has been in a position to conduct criminal investigations only since late 2002. Consequently it has no history of accessing communications data. Postcomm only requires access to postal communications data – including postal traffic data – and will be limited as such. It is likely to access communications data on about a dozen occasions per year.

56. The Gaming Board of Great Britain regulates casinos, bingo clubs, gaming machines and most lotteries. It ensures that those involved in organising gaming and lotteries are fit and proper

23 Formerly Consignia plc
24 Under the Theft Act 1986, Criminal Damage Act 1971, Forgery and Counterfeiting Act 1981 and Postal Services Act 2000

to do so, keeps gaming free from criminal infiltration, and ensures that gaming and lotteries are run fairly and legally. The Gaming Board do not currently use communications data, but anticipate a need for it based on the increasing illegal supply of gaming machines to pubs and private clubs. Suppliers usually advertise using mobile phone numbers and conduct their business through the use of those phones. Communications data would also assist in combating illegal lotteries, such as scratch cards or hoax charity appeals. Premium phone call scams are often used to facilitate both these activities; PO box numbers or other forms of postal redirection services (both of which come under the definition of communications data in RIPA) are often used in respect of illegal lotteries as well.

57. The Charity Commission is the statutory regulator of charities in England and Wales. Its aim is to give the public confidence in the integrity of charity and to ensure that charities operate within a framework that enables them to fulfil effectively the purposes for which they were set up. While the extent of deliberate fraud or dishonesty within charities is low, the Charity Commission has legal powers to investigate it when it occurs. These include both protective (they can freeze bank accounts, for example) and information gathering powers. It uses communications data – around 50 occasions per year – to identify and act against the misuse of charity property and to trace individuals involved in fundraising abuses and fraudulent appeals.

CHARITY INVESTIGATION

An animal rescue centre was investigated by the Charity Commission after a complaint was received about the treatment of animals there. The charity had persistently failed to submit accounts as required by the Charities Act 1993. As part of the investigation, the Commission obtained details of calls made from the fixed line and mobile telephones to which the charity subscribed. These showed that the trustees of the charity had been using mobile telephones to make calls for personal business, including long overseas calls, but paid for through the charity funds. As a result of this and other financial irregularities, the trustees were suspended from the charity by the Commission and a Receiver and Manager appointed to protect the remaining assets of the charity, including the animals, which were then transferred to another charity with similar purposes. The rescue centre was removed from the register of charities.

CHAPTER THREE BALANCING PRIVACY WITH PROTECTION OF THE PUBLIC

1. Any access to communications data by public authorities is an intrusion into someone's privacy. To be justified, such intrusion must satisfy the principles of necessity and proportionality derived from the European Convention on Human Rights (ECHR) and embedded in RIPA.

Necessity

2. Under section 22(2) of RIPA, communications data can be accessed only if it is necessary for one or more of the following purposes:

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic well-being of the United Kingdom (where there is a direct link with national security[25]);
- 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; or
- 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.

3. The Government does not intend to add any further purposes to this list.

Proportionality

4. It is not enough to show that access to communications data is necessary for one of the statutory purposes. Section 22(5) of RIPA requires that any access must also be proportionate to what is sought to be achieved by obtaining the data. This means that if what is proposed has a legitimate purpose but interferes with a Convention right, the interference is not justified if the means to achieve that purpose are excessive, arbitrary or unfair. Any potential collateral intrusion must also be taken into account. Even after all these considerations, interference may still not be justified if the impact on an individual or group of individuals is too severe.

Criteria

5. Based on the principles of necessity and proportionality, the following criteria must, in practice, be satisfied before any public authority can be considered for inclusion within the RIPA regime for accessing communications data:

- the authority is a public authority within the meaning of section 6(3) of the Human Rights Act[26];
- access to communications data is necessary to fulfil one or more of the statutory purposes in section 22(2) of RIPA;
- the public authority can show that it is necessary to obtain communications data in order to carry out its functions and can state what types of communications data it needs to access; and
- the access sought (taking account of the purpose for which it is needed and the type of data required) is proportionate to what it seeks to achieve (section 22(5) of RIPA).

25 See paragraph 4.2 of the draft Code of Practice for Accessing Communications Data (August 2001), www.homeoffice.gov.uk/ripa/pcdcpc.htm#Purposes
26 '… "public authority" includes (a) a court or tribunal, and (b) any person certain of whose functions are functions of a public nature, but does not include either House of Parliament or a person exercising functions in connection with proceedings in Parliament.'

Safeguards

6. There are certain safeguards that will apply to all public authorities that access communications data under RIPA. These safeguards provide further reassurance that the exercise of powers to access communications data under RIPA takes proper account of proportionality and necessity considerations, and that scope for abuse is minimised. They are:

- specifying clearly the persons designated to seek access to data;
- an accreditation scheme for certain individuals with access to communications data;
- compliance with RIPA Statutory Code of Practice;
- oversight by the Interception of Communications Commissioner; and
- sanctions for the abuse of powers to access communications data under RIPA.

Specifying clearly the persons designated to seek access

7. Under section 25(2) of RIPA, an Order is required to designate those individuals who can issue notices or grant authorisations[27] to access communications data. This can have the effect of restricting those individuals to particular posts or type(s) of posts, at particular ranks or grades, relating to particular functions of the public authority. An option is to define these as tightly as possible – for example, the Chief Inspector of Weights and Measures or a Deputy Chief Inspector in the Trading Standards Service of the Department of Enterprise, Trade and Investment for Northern Ireland (although there may be some difficulty in doing so in certain public authorities). This restricts authority to seek access to communications data within a public authority to those who require it to carry out their functions, and therefore reduces the risk of abuse of access to such data.

8. A related safeguard would be to require the designated person to have a particularly high level of seniority within the public authority. However, there is a balance to be struck. The designated person must be both senior and accountable, but equally, needs to have working knowledge of the field.

An accreditation scheme

9. An accreditation scheme, including specialised training (for example, on how the Internet works and what data a communications service provider can reasonably supply), would help ensure that individuals involved in access to communications data within each public authority apply best practice and perform to high standards. Accreditation of individuals might be limited to Single Points of Contact (SPoCs)[28]. RIPA does not include provision for accreditation, but some work on this has already been taken forward: the Association of Chief Police Officers (ACPO), with the support of communications service providers, has developed such a scheme for SPoCs working for the police, Customs and Excise, National Criminal Intelligence Service and National Crime Squad. Similarly, additional public authorities will be expected to ensure appropriate training and accreditation to standards recognised by industry; those standards should be open to public scrutiny[29]. Accreditation would promote necessary specific training and bring added reassurance.

10. In addition to ensuring that officials of public authorities meet required standards when using RIPA powers, the Government is considering with the industry and technical experts issues surrounding access to communications data under RIPA as they relate to technical and professional staff in the communications service industry. In particular, consideration is being given to procedures and processes that can be put in place to ensure professional systems that command public confidence.

RIPA statutory code of practice

11. RIPA provides for a statutory code of practice giving guidance on the procedures that

27 See annex B for a definition of these terms

28 The SPoC is an individual or group of individuals within a public authority who has been trained and accredited to facilitate lawful access to communications data and maintain effective co-operation between their authority and communications service providers.

29 Consideration may need to be given to the creation of multi-agency SPoCs for those additional public authorities that require communications data infrequently. This would require amendment of RIPA.

must be followed before public authorities can access communications data under these provisions, including guidance on:

- necessity and proportionality considerations;
- the content of an authorisation or notice requiring access to communications data;
- retention of records;
- data protection safeguards; and
- complaints.

12. A draft code of practice for Chapter II of Part I of RIPA was published for public consultation in August 2001 and remains in draft. It is available online at

www.homeoffice.gov.uk/ripa/pcdcpc.htm#Purposes.

The code will be laid before Parliament in due course.

13. This code does not prevent public authorities from maintaining and publishing their own good practice guides.

Oversight by the Interception of Communications Commissioner

14. The Interception of Communications Commissioner will provide independent oversight of access to communications data under RIPA. Appointed by the Prime Minister, he must keep under review 'the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II of Part I[30]. This is in addition to his responsibilities in relation to the interception of communications. He must report to the Prime Minister annually on the work he does, and may report at any time on matters he believes should be drawn to the Prime Minister's attention immediately. Those involved in accessing communications data are under a duty to provide him with the documents and information he needs in order to perform his role.

Sanctions

15. There needs to be transparent and credible sanctions for officials from public authorities who access communications data inappropriately or unlawfully.

16. Section 55 of the Data Protection Act 1998 makes it an offence knowingly or recklessly to obtain personal data without the consent of the data controller[31]. This offence could be committed by any official of any public authority who gained access to personal data through abuse of the RIPA provisions. Such behaviour might also be a preparatory act to a substantive offence, for example, harrassment or blackmail.

17. Legislation under which a number of public authorities operate includes criminal penalties for misconduct, including imprisonment[32]. Abuse of position can also lead to disciplinary proceedings, which can result in dismissal.

18. But there is no explicit offence under RIPA to cover deliberate, criminally-motivated misuse of the access to communications data provisions. This is an issue that may need to be addressed to send a strong signal to those entrusted to use these powers that abuse of an individual's privacy is unacceptable.

19. The abuse of individual privacy by public officials tasked with protecting the public from crime is a matter that a wider review of the balance between respect for privacy and protecting the public from crime (see chapter 4) could consider.

Getting the balance right

20. The public and Parliament expressed concerns about whether the withdrawn Order struck the right balance between intrusion into an individual's privacy and protection of the public, despite the statutory requirements of necessity and proportionality, and universally applicable safeguards. We have therefore re-examined carefully the cases made by all the public authorities seeking access to communications data, paying particular attention to the principles of necessity and proportionality through application of the criteria.

30 Section 57(2)(b) of RIPA
31 The maximum penalty is a fine of the statutory maximum on summary conviction or an unlimited fine on indictment.
32 For example, section 31 of the Health and Safety at Work Act 1974 and section 245 of the Enterprise Act 2002.

21. Giving public authorities powers they do not need is disproportionate. Equally, preventing them from fulfilling their functions to investigate crime and to protect the public by barring access to any communications data is a disproportionate response to the concerns expressed by the public and Parliament.

22. Our main conclusion is that the original Orders were too permissive. They allowed a long list of additional public authorities access to the full range of communications data. While we are satisfied that all of the additional public authorities covered by the withdrawn Order have a legitimate need to access communications data, it is not clear that in every case access to all types of communications data is demonstrably proportionate.

23. In considering the scope for a more restrictive approach under RIPA, we have identified three main options:

- the restricted access and double lock options. These options would restrict access by type of communications data and the purposes for which it is sought (restricted access) and, where appropriate, apply a further significant safeguard (a double lock) – such as prior scrutiny of applications for access to data by an independent third party. These approaches would allow only a small number of additional public authorities to have direct access to all types of communications data. The majority would only be able to access limited types of data (data about subscribers and their use of services) and, under the double lock option, only then with the approval of an independent third party; and

- the short list option. This option would allow access to communications data only to a small number of additional public authorities: police bodies and the other emergency services.

The restricted access and double lock options

24. Our review of the use of communications data by the additional public authorities leads us to conclude that a restrictive approach – enabling access to communications data for which there is a necessary and proportionate requirement – combined with further significant safeguards (a double lock), would provide greater public reassurance.

25. We have identified two potential restrictions that would form the basis for both the restricted access and the double lock options:

- restricting access by purpose (and function); and

- restricting access by type of data.

Restricting access by purpose (and function)

26. Section 25(3)(b) of RIPA permits restrictions of the statutory purposes in section 22(2) for which any public authority can access data. Thus, a new Order could restrict public authorities' access to data to specific statutory purposes only, such as 'to prevent and detect crime'. Indeed, such a restriction will be applied to those bodies such as law enforcement agencies that are already listed in the Act. It would also be possible to go further, and limit the purposes in line with a public authority's functions – for example, 'to prevent and detect crime in relation to environmental health'. This would help to ensure that public authorities access data only for legitimate purposes relating to their functions.

Restricting access by type of data

27. This would use section 25(3)(a) of RIPA to restrict the types of data each public authority can access. This could be done in the form of a blanket restriction, or be tailored to the operational requirements of each authority. Any restrictions to access by data type could be made by reference to the definitions of communications data in section 21(4), or be more specific than the legislation.

28. Tailoring the restriction to each public authority addresses directly the issue of proportionality of access. Public authorities that have no demonstrable requirement to access a certain type or types of communications data need no power to access that data. For example, for the majority of additional public authorities, access to traffic data is currently neither necessary nor proportionate to the matters they deal with. Any

restriction could be reviewed if it became clear that a public authority was able to demonstrate to Parliament that their operational requirements had changed, justifying necessary and proportionate access to a previously restricted type of data.

Double lock on restricted access

29. Simply restricting access by purpose (and function) and data type, together with the universal safeguards that will apply to all authorities using RIPA to access communications data, is a credible option. It could deliver significant reassurance that the RIPA powers to access communications data were being used appropriately. Nonetheless, we consider that an approach combining restrictions on access with additional safeguards – a double lock on access to data – better provides the level of reassurance that the public and Parliament are looking for.

30. We have identified four potential additional safeguards:

- judicial authorisation;
- prior approval by an independent third party;
- requiring the police to make requests and conduct investigations on behalf of public authorities; and
- a certification scheme for public authorities with access to communications data.

31. The double lock could be applied to certain additional public authorities or in relation to certain types of communications data. Authorities able to demonstrate a need for access to communications data but with little or no experience of doing so might gain most from the reassurance provided by a double lock.

Judicial authorisation

32. The use of judicial warranting (written authorisation by a member of the judiciary) was discussed during the passage of the Regulation of Investigatory Powers Bill through Parliament. However, Parliament chose to impose executive warranting rather than judicial warranting for the most intrusive type of surveillance – interception of communications content – in both RIPA and its predecessor, the Interception of Communications Act 1985. Parliament agreed that access to communications data was less intrusive than that activity, and accordingly did not require executive approval of that activity.

33. There appears to be consensus that granting access to the least intrusive forms of communications data, such as telephone subscriber information (which makes up 90 per cent of requests for data), would be an inappropriate and burdensome duty on the courts, both financially and in terms of time spent:

- it would delay the delivery of justice;
- it would also result in delay to investigations, when in some instances requirements for data are time-critical;
- the introduction of judicial warranting of powers under Chapter II of Part I of RIPA would be inconsistent with the rest of the Act as agreed by Parliament and which, as it stands, is compatible with Human Rights Act 1998 and ECHR obligations; and
- judicial orders under the Police and Criminal Evidence Act 1984 (PACE), in matters where it is reasonably believed a serious arrestable offence has been committed, provide for cost recovery only at the discretion of a Judge and no requirement to go via a SPoC, and so are not favoured by communications service providers.

34. Nonetheless, there remains concern that access to communications data other than service user data should require prior approval from some form of judicial body. Such an approach would provide significant reassurance to those concerned about potential abuse of powers to access communications data. If any responsibility in this area were to be transferred to the judiciary, training would need to be provided, to ensure that judges understand the issues that surround it. This would comprise not just technical knowledge but also matters such as how and why communications data is useful, the resource implications of a requirement for communications data, and so on.

Prior approval by third party

35. Additional public authorities could submit requirements for access to communications data, other than subscriber data, to an independent

third party for prior approval. This would be an administrative arrangement, as there is no statutory provision for it in Chapter II of Part I of RIPA. The third party could assess the consideration of necessity and proportionality made by the public authority, and make a judgement whether or not the public authority should proceed with the required access.

36. The Office of the Interception of Communications Commissioner could fulfil this role. If so, appropriate additional resources would be provided. The Office of the Surveillance Commissioner performs a similar function, albeit a statutory one, in granting or refusing approval for certain authorisations for interference with property under the Police Act 1997 and intrusive surveillance under Part II of RIPA.

37. This form of oversight potentially provides additional reassurance that powers under RIPA were being exercised appropriately. There is a clear benefit in defective requirements for access to data being identified and any unnecessary or disproportionate intrusion into privacy prevented. Although it would not be statutory, it could be provided for in a code of practice. We consider it unlikely that a designated person would go against the advice of an independent third party. But this approach could give rise to certain issues:

- involvement of an independent third party might be seen to blur the clear responsibility of a designated person for issuing notices and granting authorisations to access data, and obscure liability if access made with the approval of an independent third party was found to be defective; and

- if the Office of the Interception of Communications Commissioner were to act as the independent third party, there could be scope for confusion between the Commissioner's roles for statutory oversight and non-statutory prior approval.

Requiring the police to make requests and conduct investigations on behalf of public authorities

38. Requiring the police to conduct specialist criminal investigations that are currently undertaken effectively by public authorities in central and local Government would have a number of implications:

- in many cases it would be a distraction from the core functions and responsibilities of the police, as set out in documents such as the national policing plan[33];

- the police lack the expertise to investigate properly many of the specialist crimes that fall to these public authorities. Indeed, the Police Reform Act 2002 specifically gives police powers to civilian investigators who will be better equipped to investigate certain, specialist forms of crime;

- it would also add a significant additional burden to police forces, at a time when the Government is making a concerted effort to focus police resources on crime prevention and detection that cannot properly be undertaken by others; and

- ultimately, it could undermine the wider law enforcement work undertaken by these additional authorities and the powers they have been given over the years by Parliament.

39. Requiring the police to conduct all investigations that involve communications data might therefore seem a disproportionate response to the concerns that have been expressed about other public authorities having access to that data.

A certification scheme for public authorities with access to communications data

40. Certification would cover the processes for recording decisions about access to communications data and actions relating to the use, storage and destruction of data within a public authority as a whole. (Accreditation would cover an individual's part in the process within that authority.)

41. A prerequisite to continued use of powers to access communications data could be some form of certification. Additional public authorities could be given a twelve-month probation period after passage of a new Order to ensure that they were satisfactorily complying with all the

33 www.policereform.gov.uk/natpoliceplan.asp

requirements. Certification could be renewable annually.

42. Certification would provide a positive public statement that each individual public authority was meeting required standards. The Interception of Communications Commissioner is under a duty to keep the use of Chapter II of Part I of the Act under review and submit an annual report to the Prime Minister about the carrying out of his functions. Certification decisions might be taken by the Commissioner or be based upon his reports. He could advise the Home Secretary if he believed a public authority needed to be removed from the Order.

The short list option

43. An alternative to the options giving restricted access to a number of additional public authorities is a short list, which would restrict access to communications data to police bodies and other emergency services. This approach has advantages:

- it is clear and unequivocal;
- the investigation of serious crime, protection of national security and saving of life in emergencies clearly satisfy the proportionality test; and
- it would address directly the concern that powers to access communications data should not be widely available to public authorities, providing reassurance that the scope for abuse is limited.

44. This short list option would come at a price:

- it would adversely affect the ability of many public authorities to prevent and detect serious and less serious crimes that impact upon local communities and matter to the public;
- Parliament has expressly given specific functions to these public authorities to investigate such crimes rather than the police;
- where public authorities excluded from the RIPA regime investigate serious crime, the police would have to become involved in the investigation;
- it would inevitably pressure the police to become involved in investigations of less serious crimes, which though important to the public, are not policing priorities (as explained in paragraph 38);
- taken to its logical conclusion, it could lead to calls for law enforcement and intelligence agencies to be restricted in this way, leaving no one able to investigate less serious crimes where communications data provides vital evidence; and
- to the extent public authorities not included within the RIPA regime were able to use other legislation to access communications data, it would undermine one of the main purposes of RIPA: the creation of a single ECHR compliant regulatory regime for such access.

45. We believe this approach has flaws. It would perpetuate uncertainty about the regime to access communications data with regard to less serious crime, rather than place it in a single regulatory regime. It would also lead to inefficient and ineffectual investigations of those crimes, and would not best serve the victims of those crimes or communities affected by those crimes.

Implementing a communications data access regime for additional public authorities

46. A small number of public authorities – police bodies and other emergency services –have made the strongest case for regulated access to all types of data, primarily for the investigation of serious crime, protection of national security or provision of emergency services. They are:

- Ambulance Service NHS Trusts: *emergency ambulance services*
- fire authorities
- Department for Transport: *Maritime and Coastguard Agency*
- Scottish Drugs Enforcement Agency
- United Kingdom Atomic Energy Authority Constabulary

47. For these authorities, the purposes for which the data is required would be frustrated if any

type of data were inaccessible or access subject to a double lock. Such authorities would be likely to comprise the short list, if that approach were adopted.

48. A larger number of additional public authorities have demonstrated a necessary and proportionate requirement for access to service use and subscriber data, but not traffic data[34]. They are:

- Common Services Agency for the Scottish Health Service: *NHSScotland Counter Fraud Services*
- Department of Enterprise, Trade and Investment for Northern Ireland: *Trading Standards Service*
- Department for Environment, Food and Rural Affairs: *Investigation Branch; Centre for Environment, Fisheries and Aquaculture Science; Counter Fraud and Compliance Unit of the Rural Payments Agency*
- Department of Health: *Medicines Control Agency; Medical Devices Agency*
- Department of Trade and Industry: *Companies Investigation Branch; Legal Services Directorate D; Radiocommunications Agency*
- Department for Work and Pensions: *Counter Fraud Investigation Division (Operations); Counter Fraud Investigation Service*
- Environment Agency
- Financial Services Authority
- Food Standards Agency
- Gaming Board of Great Britain
- Health and Safety Executive
- Home Office: *Immigration Service (Enforcement Directorate and Intelligence Directorate)*
- Information Commissioner
- local authorities: *trading standards, environmental health, housing benefit and planning functions*
- NHS Counter Fraud and Security Management Service
- Northern Ireland Central Services Agency for Health and Social Services: *Counter Fraud Unit*
- Office of Fair Trading: *Cartel Investigation Branch*
- Postal Services Commission (Postcomm has a unique requirement for postal service communications data only – including postal traffic data)
- Royal Mail Group plc
- Scottish Environment Protection Agency
- Serious Fraud Office

49. We consider that access to communications data by these authorities should be restricted by type of data and, where appropriate, subject to certification and prior scrutiny by an independent third party – our initial view is that these should be by the Office of the Interception of Communications Commissioner.

50. The Government recognises that criminal activity is constantly changing, and that consequently the data access requirements of public authorities may change too, particularly as less serious crime (for example, consumer fraud) increasingly goes online. In the future, where a public authority could demonstrate a necessary and proportionate requirement to access traffic data that access might be permitted subject to third party prior approval. Equally, a public authority that has consistently demonstrated to the Interception of Communications Commissioner and the public that it uses RIPA powers to access communications data appropriately might be released from a requirement for prior scrutiny of all or some of its requirements for data. There will be a constant need for the Government to keep the use of the powers under review and to seek Parliamentary approval for any necessary change to the data access regime, and for the Interception of Communications Commissioner to monitor whether public authorities access communications data appropriately.

Seeking your views

51. The Government seeks views on the options and safeguards described in this chapter for enabling additional public authorities to access communications data under RIPA. In particular, we welcome comments on how best to meet additional public authorities' necessary and proportionate requirements for communications data in a way that commands public confidence.

CHAPTER FOUR STRIKING THE RIGHT BALANCE: RESPECTING THE PRIVACY OF INDIVIDUALS AND PROTECTING THE PUBLIC FROM CRIME

1. Widespread public concern about the Government's proposals for public authorities' access to communications data may have been a "lightning rod" for a wider set of concerns about how the Government strikes the delicate balance between upholding the rights of individuals and interfering with those rights in the public interest.

2. In view of those wider concerns set against the changes taking place in modern society that have the potential to undermine individual privacy, the Home Secretary said:

> *The reaction to our plans has shown that we need a much broader public debate about how to strike the balance between the privacy of the individual and society's legitimate need for measures to support the investigation of crime and to protect the public*[35].

3. In an information society – a world full of data – the issues of privacy and personal data have risen up the political agenda, particularly in the context of law enforcement and public safety. The volume of personal data we generate and is generated about us and about our lives is increasing. Data and identity are increasingly linked. The marketing, targeting and delivery of services in the public and private sectors are being transformed, as are the ways in which crime can be committed. With our identity in our data there is, equally increasingly, the scope for us to be misrepresented or harmed by misuse or abuse of that data. This is a new aspect of life.

4. The challenge for Government is to protect and uphold privacy, so far as possible, at the same time as enabling law enforcement to intrude into privacy in a way that does not undermine public trust and support for law enforcement work. This requires widely shared understanding and reassurance that intrusion of privacy is undertaken only when necessary and proportionate and is subject to strict oversight, and that unjustified privacy violation by those entrusted to do it lawfully can represent a crime equally serious as one meriting lawful intrusion of privacy.

5. There is a relationship between privacy and freedom. We value our privacy. We value our freedom. In the same way our freedom is balanced against society's rules, our privacy has to be balanced against the needs of society for preventing and detecting crime.

What are the privacy concerns?

6. The Government recognises there are concerns about privacy invasive techniques used in the public interest to prevent and detect crime and protect the public.

7. Since the withdrawal of the Order last summer, we have received comments from the public and from individuals and organisations concerned with privacy and data protection issues made in correspondence to the Home Office and in online discussion groups.

8. The privacy issues and concerns being expressed to Government (summarised in annex C) are about the authorisation, use and oversight of lawful intrusion into privacy to prevent and detect crime and protect the public, and sanctions for any abuse of those powers. They also include the concern that the development and use of increasingly sophisticated surveillance technologies should be accompanied by appropriate regulation and safeguards, and concerns around the "secrecy of surveillance".

9. Public concern about the use of privacy invasive methods for the purpose of law enforcement, national security and public safety needs to be addressed and, so far as possible, allayed through clear explanation of the public benefits. Knowledge of processes helps ensure there are no misconceptions about the work of public authorities on behalf of the public.

35 Home Office Press Notice (18 June 2002) www.gnn.gov.uk/gnn/national.nsf/HO/C0BDE2541EAA9D4280256BF3005AFDB0?opendocument

A need for public debate?

10. The Government is committed to privacy and the protection of personal information used in delivering services to the public[36], including those provided by law enforcement agencies and public authorities having law enforcement and public safety functions.

11. The PIU report "Privacy and data-sharing" set down the principle that where personal information or data is used without the consent of the individual, there should be 'openness, transparency and consultation in the policy-making process of striking a balance between individual rights and the wider public interest.'[37] This principle is directly relevant to the development, and elaboration, of policy around intrusion into privacy for the purposes of prevention and detection of crime and public safety.

12. The need for public authorities tasked with law enforcement and public safety functions to intrude on an individual's privacy where necessary and proportionate in the wider public interest is, however broadly interpreted, not in dispute.[38] What is at issue is the circumstances in which it should be permitted to take place, the scrutiny to which it is subject, the degree of openness associated with it and the sanctions attached to the abuse of the power of intrusion.

13. In circumstances where intrusion into privacy is possible, it should be clear what information is accessible by whom, for what purpose, how the information is protected, and what redress and oversight mechanisms are in place if things go wrong. Those who then engage in conduct, knowing from information placed in the public domain, that as a consequence their privacy is liable to compromise, accept the risk to their privacy.

14. So where should the balance lie between matters that are private and should remain so, and matters that are private but should be intruded upon in the public interest to prevent or detect crime or to protect the public? And how should that balance be operated and maintained?

Seeking your views

15. The Government invites views on the need for a wider review of the balance to be struck between privacy and protecting the public from crime. If there is such a need, what questions might that review address?[39]

36 Performance and Innovation Unit report *Privacy and data-sharing The way forward for public services (April 2002)* www.cabinet-office.gov.uk/innovation/2002/privacy/report/index.htm
37 Performance and Innovation Unit report Privacy and data-sharing, p.5
38 Examples of lawful intrusions into privacy are contained in Annex D
39 See Annex E for some suggestions

ANNEX A **THE INDEPENDENT PANEL OF EXPERTS**

1. We are grateful for the help of the following independent experts in writing this consultation document:

Madeleine Colvin	Barrister, Human Rights Consultant and former Director of Legal Policy at JUSTICE
Stewart Dresner	Chief Executive, Privacy Laws & Business
Dr. Ian Kearns	Head of the Digital Society Programme, Institute for Public Policy Research
Danny Meadows-Klue	Chief Executive, Digital Strategy Consulting Limited
James Michael	Senior Research Fellow, Institute of Advanced Legal Studies, University of London and Visiting Professor at the University of Cape Town

2. We have benefited from the advice of the independent experts, and from the participation of representatives of the Confederation of British Industry and the Trades Union Congress in our discussions to prepare this paper, but the views expressed in this document are those of the Home Office.

ANNEX B **LEGAL FRAMEWORK**

1. Any public authority can only obtain or disclose information to the extent that it has statutory or common law powers to do so and such powers are constrained by other legal considerations, such as the Human Rights Act 1998 or the requirements of the Data Protection Act 1998.

Human rights law

2. The European Convention on Human Rights (ECHR), in Article 8, asserts both the right of individuals to have their privacy respected and that public authorities may lawfully interfere with that right in certain lawful and clearly demonstrated circumstances.

> *Everyone has the right to respect for his private and family life, his home and his correspondence.*[40]
>
> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*[41].

Privacy, therefore, is a fundamental human right, but not an absolute right.

3. Article 6 of ECHR – the right to a fair trial – is also relevant. It applies to fairness at investigative stage too, to the extent that that affects any resulting trial or evidence.

4. The Human Rights Act 1998 (HRA) incorporated the Convention into domestic law, allowing individuals to assert their rights under the Convention in UK courts. Section 6 of the Act provides that 'it is unlawful for a public authority to act in a way that is incompatible with a Convention right'.

Data Protection Act 1998

5. The Data Protection Act 1998 (DPA) regulates the processing and handling of personal information that has been obtained lawfully. All processing of personal data, including disclosure of communications data, whether under RIPA or any other statutory or common law regime, must also comply with the requirements of the DPA.

6. Communications service providers (CSPs) need to ensure that personal data is disclosed for a purpose other than that for which it was provided only if the person consents, if there is a legal requirement to make the disclosure or if there is an overriding public interest in making it. The DPA provides a general restriction on disclosure but makes exemptions to the general restriction on disclosure, such as for safeguarding national security (section 28), where failure to disclose would be likely to prejudice crime prevention or detection or the apprehension or prosecution of offenders (section 29) or where disclosure is required by law, or necessary in connection with legal proceedings (section 35).

7. In the case of communications data, a public authority requests data from the relevant CSP, using mutually agreed procedures, and the CSP can choose to provide it – but is not obliged to do so. Where an exemption is properly applied, the disclosure will not breach the DPA. However, exercising an exemption confers no immunity from the requirements of other law and a CSP breaching any other relevant law in making the disclosure, such as the common law duty of confidence, would still be liable to legal action.

40 Article 8.1, European Convention of Human Rights

41 Article 8.2, European Convention of Human Rights

Although the public authority must consider the necessity and proportionality of any request, it is the CSP that is liable if the disclosure of data is challenged in courts. Consequently, the CSP must also have regard to the request for data in the light of those human rights requirements, even though they are not best placed to do so. CSPs can and do turn down requests if they have doubts about its necessity or proportionality, in which case the public authority goes without the data or, if it is able to, seeks a court order.

8. The liability of CSPs for the disclosure of communications data has led some CSPs to indicate that, once RIPA has been implemented, they will be reluctant to continue exercising their discretion to disclose information to any public authority on the basis of overriding public interest.

9. Public authorities and CSPs co-operate to ensure that disclosures of data are compliant with the DPA. The public authorities currently listed in RIPA each have an accredited Single Point of Contact (SPoC) through whom all requests are routed. This ensures that CSPs do not receive requests from many different individuals within one organisation, and that requests are of a consistently satisfactory standard, and only for data that the CSP can reasonably provide. Accreditation is achieved through participation on a training course developed jointly by ACPO and CSPs.

Statutory powers to seek disclosure of communications data

10. Several public authorities have an ability to require production or disclosure of information in general and use this to access communications data, for example:

- a Production Order authorised by a Circuit judge under the Police and Criminal Evidence Act 1984 (PACE) in relation to evidence of serious offences – used by the police, customs and the Legal Services Directorate of the DTI;
- section 1 of the Social Security Fraud Act 2001 contains specific provisions to access communications data (other than traffic data) for authorised Department for Work and Pensions and authorised local authority staff conducting investigations relating to fraud against the benefit system; and
- the Charities Act 1993 (used by the Charity Commission), the Criminal Justice Act 1987 (used by the Serious Fraud Office), the Environmental Protection Act 1990 (used by the Environment Agency and local authority environmental health officers), the Financial Services and Markets Act 2000 (used by the Financial Services Authority and the DTI Companies Investigation Branch) and the Health and Safety at Work Act 1974 (used by the Health and Safety Executive).

Regulation of Investigatory Powers Act 2000 (RIPA)

11. The Regulation of Investigatory Powers Act 2000 (RIPA) provides for lawful interception of communications (disclosure of contents of communications), access to communications data (disclosure of data about communications), covert surveillance, and access to protected electronic data. It also provides for independent oversight of the use of those powers and a means of redress for those affected by their misuse.

12. RIPA was introduced for two reasons:

- to regulate, and make compatible with human rights legislation, the use of various investigatory powers by those involved in law enforcement; and
- to ensure that those involved in preventing and detecting crime have the powers to fulfil their role effectively in an age of rapid technological change.

Part I Chapter II of RIPA

13. The purpose of Chapter II of Part I of RIPA is to introduce a single, clear statutory framework for the requisition of communications data by public authorities. In accordance with ECHR requirements, it makes specific reference to necessity (access to communications data must be necessary for fighting crime or another RIPA-defined purpose) and proportionality (the extent of any necessary access to data must be proportionate to what that access seeks to achieve).

14. Under RIPA liability for taking proper account of necessity and proportionality of any disclosure lies with the public authority seeking access, not the CSP.

15. Unlike many statutory information-gathering powers used to access communications data, the exercise of these powers under RIPA is subject to specific oversight – by the independent Interception of Communications Commissioner[42]. The independent Investigatory Powers Tribunal provides a complaints mechanism for those who feel their communications data has been accessed unnecessarily or disproportionately.

16. Unlike other information-gathering powers, RIPA expressly provides for contribution to the costs incurred by CSPs in providing communications data to public authorities.

What is communications data?

17. Section 21 of RIPA includes an explanation of what the term 'communications data' means:

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

18. It does not include the contents of the communication itself, such as speech, correspondence, music or images. Access to the content of communications – lawful interception of communications – is covered by Chapter I of Part I of RIPA and only takes place with the authority of the Secretary of State, on an application from the most senior individuals in a limited number of authorities.[43] The Government does not intend to add to this list of individuals. This consultation paper does not cover the content of communications.

Traffic data

19. Traffic data includes:

- information identifying the sender and recipient (including copy recipients) of a communication;
- information identifying any location of a communication (such as mobile phone cell site location data);
- routing information identifying or selecting any apparatus (such as equipment, machinery or device, or any wire or cable) through which a communication is transmitted – for example, dynamic IP address allocation, web postings and e-mail headers (to the extent that content of the communication is not disclosed – the subject line of an e-mail is considered content);
- information written on the outside of a postal item (such as a letter or parcel);
- call detail records for specific calls (such as calling line identity);
- web browsing information (to the extent that only the host machine or domain name (web site name) is disclosed. For example, within a communication, data identifying **www.homeoffice.gov.uk** would be traffic data, whereas data identifying **www.homeoffice.gov.uk/kbsearch?=ripa+traffic+data** would be content);
- online tracking of communications (including postal items and parcels); and
- signalling information and dialling sequences that affects the routing of a communication (but not the delivery of information), in the investigation of "dial thru" fraud.

Service use information

20. Service use information includes data such as:

- itemised telephone call records (numbers called);

42 The Information Commissioner exercises oversight of the workings of the DPA as a whole, including the exercise of the exemptions on disclosure in matters relating to the prevention and detection of crime.

43 The Director-General of the Security Service; the Chief of the Secret Intelligence Service; the Director of Government Communications Headquarters; the Director General of the National Criminal Intelligence Service (through whom English and Welsh police forces with the exception of the Metropolitan Police apply); the Commissioner of the Metropolitan Police; the Chief Constable of the Police Service of Northern Ireland; the Chief Constable of any Scottish police force; the Commissioners of Customs and Excise; the Chief of Defence Intelligence; and a person who is the competent authority of a country or territory outside the UK for the purposes of any designated international mutual assistance agreement.

- itemised connection records;
- itemised timing and duration of service usage (calls and/or connections);
- information about the connection, disconnection and reconnection of services;
- information about the provision and use of forwarding/redirection services (by postal and telecommunications service providers);
- information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services; and
- records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

Subscriber information

21. Subscriber information includes:

- service user information (known as 'subscriber checks' or 'reverse look ups') such as "who is the subscriber of phone number 012 345 6789?", "who is the subscriber of e-mail account xyz@xyz.anyisp.co.uk?" or "who is the subscriber or who is entitled to post to web space www.xyz.anyisp.co.uk?";
- service users' account information, including payment method;
- addresses for installation and billing; and
- abstract personal records provided by subscriber to service provider (such as demographic information or sign-up data (to the extent that password or personalised service access information is not disclosed)).

Relevant public authorities

22. The RIPA access to communications data provisions may only be used by 'relevant public authorities' listed in section 25(1) of the Act or subsequently added by an Order approved by Parliament. Those listed in the Act are:

- a police force (as defined in section 81(1) of the Act);
- the National Criminal Intelligence Service;
- the National Crime Squad;
- HM Customs and Excise;
- the Inland Revenue;
- the Security Service;
- the Secret Intelligence Service; and
- the Government Communications Headquarters.

23. It was an Order to add public authorities to that list which was widely criticised by the public and Parliament in June 2002. The Home Secretary withdrew that Order to facilitate wider consultation before bringing forward new proposals.

24. RIPA tightly defines the circumstances in which communications data can be accessed. Public authorities can access communications data only if it is necessary for one or more of the following purposes and relevant to their functions:

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic well-being of the United Kingdom (where there is a direct link with national security[44]);
- 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,

44 See paragraph 4.2 of the draft Code of Practice for Accessing Communications Data (August 2001), www.homeoffice.gov.uk/ripa/pcdcpc.htm#Purposes

contribution or charge payable to a government department; or

- 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.

25. The Government does not intend to add any further purposes to this list.

26. It is not enough that access to communications data is necessary for one of the statutory purposes. Section 22(5) of RIPA requires that any access must also be proportionate to what is sought to be achieved by obtaining the data. This means that lawful access cannot be excessive, arbitrary or unfair. Potential collateral intrusion must also be taken into account.

27. Within a public authority, a 'designated person' must ensure that he is satisfied that the requirement for communications data (made by persons from the same organisation) is both necessary and proportionate before granting an authorisation or issuing a notice. (In contrast, the DPA does not require a designated person to scrutinise requests for disclosure of data). The oversight of the designated person ensures that investigators cannot easily access communications data inappropriately. The seniority of designated persons within an authority must be specified in an Order subsequent to one adding that authority to the RIPA regime.

28. The designated person can authorise access to communications data in one of two ways: an authorisation (under section 22(3)) or a notice (under section 22(4)).

29. An authorisation allows the relevant public authority to obtain data directly. This may be suitable where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data[45]; or
- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself; or
- there is a prior agreement in place between the relevant public authority and the postal or telecommunications operator to appropriate mechanisms for the disclosure of communications data.

30. A notice is given to a communications service provider, who is required – provided it is reasonably practicable to do so – to collect or retrieve the data and provide it to the designated person or another specified individual within the same public authority.

31. Both notices and authorisations are valid for a maximum of one month, though they can be renewed. They must be cancelled if they are no longer necessary or proportionate.

32. Although not a requirement under RIPA, the Home Office will insist that all notices should be channelled from relevant public authorities to CSPs via a Single Point of Contact (SPoC)[46]. This will provide for an efficient regime, since the SPoC will provide self-regulation within the public authority and by dealing with CSPs on a regular basis provide certainty of process for them. Where appropriate, SPoCs should be in a position:

- to assess whether access to communications data in a particular case is reasonably practical for the CSP;
- to advise investigators and designated persons on the practicalities of accessing different types of communications data from different CSPs;
- to advise investigators and designated persons on whether specific communications data falls under section 21(4)(a), (b) or (c) of the Act;
- to assess any cost to and resource implications for both the public authority and the CSP; and

45 Wherever possible, this assessment will be based upon information provided by the relevant communications service provider.
46 The SPoC is an individual or group of individuals within a public authority who has been trained and accredited to facilitate lawful access to communications data and maintain effective co-operation between their authority and CSPs.

- to provide a safeguard for CSPs that authorisations and notices are authentic.

33. Under section 24 of RIPA, there is a statutory duty on the Government to ensure arrangements are in place to make appropriate contributions to the costs CSPs incur in complying with notices. This does not introduce anything new, as has been standard practice to provide such payments to communications service providers. The Government considered it necessary to state clearly on the face of the Act its intention to allow this practice to continue.

34. A statutory code of practice will provide further clarification of the provisions of Chapter II of Part I of RIPA. The code will relate to the powers and duties conferred or imposed under that Chapter and provide guidance on the procedures that must be followed before access to communications data can take place under those provisions. The code will be admissible in evidence in criminal and civil proceedings. The code has not yet been finalised, but an early draft is available at

www.homeoffice.gov.uk/ripa/pcdcpc.htm#Purposes

35. The draft code of practice lays out in detail the application process for access to communications data. Applications must be in writing and include:

- information specifying the individual to whom the data relates, the exact data required and the timescale within which the data is needed;

- the reason why obtaining the required data is considered to be necessary for one or more of the statutory purposes for access; and

- an explanation of why obtaining the data is proportionate to what is sought to be achieved – including consideration of collateral intrusion, if appropriate.

36. The draft code requires records to be kept. It also specifies that where authorisations have been improperly obtained or notices improperly given, a report and explanation be sent to the Interception of Communications Commissioner.

ANNEX C **PRIVACY CONCERNS FOR A BROADER DEBATE**

1. Drawing directly from comments made to the Government in correspondence and online discussion groups since June 2002, the following concerns have been raised by members of the public about issues around lawful intrusion into privacy:

a) Privacy is increasingly becoming a more fundamental principle of society, given the potential for privacy to be destroyed by current (and future) technologies. Equally, some technologies will help preserve privacy.

b) Getting the right legal framework that treats privacy as a valuable commodity and properly addresses criminal abuse of privacy is important. Sanctions or penalties for abuse of privacy invasive techniques or abuses of power are insufficient or absent (and the sort of punishment for such abuse needs to be considered).

c) Any intrusion into privacy must be, and seen to be, proportionate to the offence (or the matter) under investigation and only undertaken when necessary to do so.[47] Processes should exist to ensure that those who engage in crime forfeit their right to be left alone (proportionately) but equally need to be counter balanced by processes to ensure that those who do not engage in crime do not forfeit their rights (disproportionately) and receive redress when their rights are violated.

d) There is concern about "purpose-creep", where data acquired for one law enforcement purpose is used for another.

e) The Government and, to varying degrees, law enforcement agencies and public authorities, do not command the full trust of the public in their use of powers that intrude into privacy. In particular, there is concern that insufficient account is taken of abuse of those powers. Examples exist where personal information has been disclosed, without respect for individual privacy.

f) There is concern that some intrusive surveillance activity can be authorised lawfully within the agency conducting the activity, and concern about whether levels of authorisation are appropriate.

g) Enabling a wide range of public authorities to undertake lawful invasion of privacy inevitably means less control over the use of those powers. Access to such powers should be graduated according to the degree of intrusion, and the courts (or a central agency representing the public interest) should be involved in the authorisation of intrusive surveillance either for all intrusion or for that over and above a certain low level of intrusion.

h) Legislation relating to conduct of intrusive activity should be brought together (and legacy legislation repealed) and made ECHR compliant. [48]

i) Oversight arrangements must be effective and provide a real disincentive to abuse of powers, combining adequate prior approval (to prevent intrusions that would be disapproved by any post-event scrutiny) with post-facto scrutiny (or publication) to prevent "correction" of records after the event. Without a trusted, effective and open regime for oversight, there is concern that mass surveillance (or arbitrary surveillance) of the population will take place unchallenged.

j) Surveillance activity is too secretive and there is insufficient public accountability,

47 This represents a degree of broad consensus on the interpretation of when public authorities should be permitted to intrude into a person's private life to investigate crime or to protect the public. How far they should do so and in what circumstances is set against the subjective concept of proportionality.

48 At issue, for example, is public authorities' future use of statutory or common law powers alongside the Data Protection Act to seek disclosure of personal information.

appropriate to a democratic society, about the extent to which it is undertaken. The circumstances in which lawful intrusion of privacy is possible, together with information about what can be done if things go wrong, should be clear, open to public scrutiny and be accessible to all sections of the community – not just the technically literate and privacy literate. Information about the processes of lawful intrusion and the extent to which lawful surveillance is conducted should be in the public domain (not least to ensure exposure of abuse or corruption).

k) Surveillance can protect the public but equally surveillance – if unchecked – can undermine people's safety (where private sensitive information is gathered and abused or distributed to those who abuse their access to it).

l) Surveillance can intrude into the privacy of individuals not under investigation.[49]

m) Targets of surveillance are not automatically notified they have been a target of surveillance and may never know (and as such mechanisms are needed that would require disclosure of the fact that intrusion has taken place, subject to safeguards – for example, disclosure after a set period of time). As one writer put it, 'If someone is important enough to monitor [i.e. be monitored], they should be important enough to be told and told why.'

n) The collection of data about everyone, on the off chance they may become a suspect, is less productive and more intrusive than collecting data about suspects.

o) There are concerns that legislation is failing to adapt to changing technology and that concepts which have evolved from fixed line (circuit switched) telephony cannot be extended easily to modern digital (packet switched) communications.

p) Data about an individual's web access can provide a far fuller insight into their activities, views, interests and contacts than a telephone log (and is far more likely of itself to contain material providing blackmail opportunities than telephone service use records). New technologies are enabling the possibility of searching various data sources to draw together unrelated personal information to create new information about an individual that represents an intrusion into privacy (about that individual's associations and movements).[50]

q) Increasing sophistication of CCTV and similar systems – automatic face recognition (AFR)[51], automatic number plate recognition, night-vision, long range vision and archiving of images – all give rise to privacy concerns, as do the levels of supervision and oversight of CCTV operations and redress for misuse of CCTV to conduct unlawful surveillance.

r) There are privacy concerns about databases (of offenders, of DNA profiles, of fingerprints) used by public authorities for public protection and the need for clear regulations about these records, access to them, their use, disclosure, retention and deletion and the opportunity to check their accuracy and to correct errors.

s) There are privacy concerns about the use, supervision and maintenance and the potential future storage of a range of biometric or digitised data (such as retina scans, body geometry, facial images, signatures or voice patterns) without suitable safeguards.

49 Concern about any collateral intrusion that takes place.

50 Data sharing (or data transfer) takes place between public authorities (the subject of the recent PIU report), including statutory information gateways, and from public to private bodies and vice versa (for example, between law enforcement agencies and financial institutions/airlines and airports/communications service providers).

51 There are particular concerns about AFR false positives (identification of the "wrong" people) and false negatives (misidentification of the "right" people).

ANNEX D **ISSUES OF INTRUSION FOR A BROADER DEBATE**

1. There are a variety of ways in which public authorities responsible for public protection can, or seek to, impact on privacy (all subject to various statutory safeguards and oversight), which might be within the scope of a broader review of privacy and protecting the public from crime, as proposed in chapter four:

a) Interception of communications[52] – covert interception of the content of communications (whether by phone, e-mail or post), generally regarded as the most intrusive form of surveillance.

b) Intrusive surveillance[53] – including covert observation and eavesdropping on conversations in private spaces (premises or vehicles), and covert interference with property[54].

c) Directed surveillance[55] – covert unintrusive surveillance, for example observation and eavesdropping on conversations in public spaces and vehicle location tracking.

d) Acquisition of communications traffic data[56].

e) Acquisition of communications service use data[57].

f) Acquisition of communications service user data[58].

g) Provision for retention of communications data[59].

h) Disclosure of cryptographic key material – legislation is in place (although not yet in force) providing for the compulsory disclosure of lawfully acquired protected or encrypted information in an intelligible form or for the means (the key) to put protection information in an intelligible form[60].

i) CCTV – widespread use of overt closed circuit television in private and public places, and evidence from CCTV images in some high profile enquiries into crime and terrorism, has largely met with acceptance from the public. In July 2000, the Data Protection Commissioner issued a Code of Practice under the Data Protection Act 1998.[61] The Code makes clear to operators of CCTV systems their legal obligations and provides reassurance to the public about the safeguards that operators should have in place. Although not a strict legal requirement the Code represents good practice.

j) Automatic Face Recognition – combined with CCTV, this is developing software that can match patterns of stored digitised facial images to identify automatically, in real time, faces caught on camera against records of known persons (offenders or suspects). As with basic CCTV, the privacy impact can be addressed through regulations about appropriate use and safeguards to prevent misuse.

k) Access to private records – law enforcement agencies have long sought lawful access to private records such as financial records and employment records to assist with enquiries. The Bankers Books Evidence Act 1879 and more recently the Police and Criminal Evidence Act 1984 and the Criminal Justice Act 1987 have provided a basis for access to financial and business records held in confidence.

52 Part I Chapter I, Regulation of Investigatory Powers Act 2000
53 Section 26(3), Part II, Regulation of Investigatory Powers Act 2000
54 Section 5, Intelligence Services Act 1994 and Part III, Police Act 1997
55 Section 26(2), Part II, Regulation of Investigatory Powers Act 2000
56 Sections 21(4)(a) and 21(6) Part I Chapter II, Regulation of Investigatory Powers Act 2000 (not in force)
57 Section 21(4)(b) Part I Chapter II, Regulation of Investigatory Powers Act 2000 (not in force)
58 Section 21(4)(c) Part I Chapter II, Regulation of Investigatory Powers Act 2000 (not in force)
59 Part 11, Anti-Terrorism, Crime and Security Act 2001
60 Part III, Regulation of Investigatory Powers Act 2000 (not in force)
61 www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def30802566360045bf4d/db76232b37b5bb648025691900413c9d?OpenDocument

ANNEX E **QUESTIONS FOR A BROADER DEBATE**

a) Is there a contradiction between an expectation of respect for individual privacy ("your privacy") and an expectation of necessary and proportionate intrusion into the privacy of those acting contrary to the public interest ("someone else's privacy")?

b) What protections for privacy can and should the citizen expect to be in place in order to maintain a healthy balance between his own privacy and his interest in a society safe from crime?

c) When, and how far, should public authorities be permitted to intrude into a person's private life to investigate crime or to protect the public?

d) How can law enforcement agencies and other public bodies with law enforcement functions secure the trust of the public in their use of privacy invasive techniques?

e) How can the public benefit in interfering with privacy rights be demonstrated?

f) How can detrimental effects on privacy be addressed and, wherever possible, mitigated? What alternatives are there?

g) How can reassurance be provided publicly about the conduct of ongoing and proposed privacy-invasive activities?

h) Should unlawful privacy violation, by criminals or law enforcers, be acknowledged clearly as a crime? Are current powers for criminal violation of privacy too limited?

ANNEX F **CONSULTATION CRITERIA**

1. The Government's code of practice on written consultation[62] sets out criteria that should apply to all national public consultations:

- Timing of consultation should be built into the planning process for a policy (including legislation) or service from the start, so that it has the best prospect of improving the proposals concerned, and so that sufficient time is left for it at each stage.
- It should be clear who is being consulted, about what questions, in what timescale and for what purpose.
- A consultation document should be as simple and concise as possible. It should include a summary, in two pages at most, of the main questions it seeks views on. It should make it as easy as possible for readers to respond, make contact or complain.
- Documents should be made widely available, with the fullest use of electronic means (though not to the exclusion of others), and effectively drawn to the attention of all interested groups and individuals.
- Sufficient time should be allowed for considered responses from all groups with an interest. Twelve weeks should be the standard minimum period for a consultation.
- Responses should be carefully and open-mindedly analysed, and the results made widely available, with an account of the views expressed, and reasons for decisions finally taken.
- Departments should monitor and evaluate consultations, designating a consultation co-ordinator who will ensure the lessons are disseminated.

62 www.cabinet-office.gov.uk/servicefirst/2000/consult/code/ConsultationCode.htm