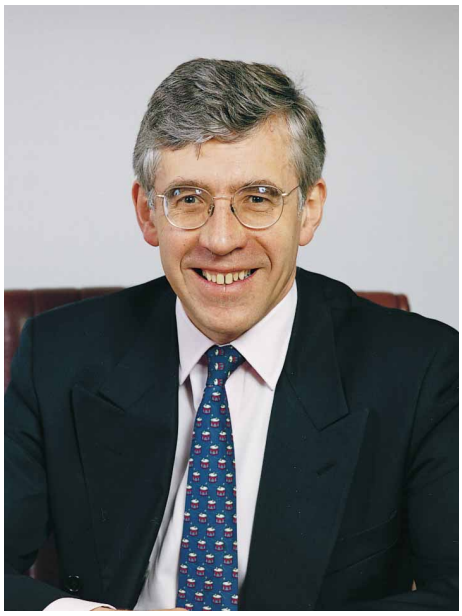
Interception of Communications in the United Kingdom

A consultation paper

Presented to Parliament by the Secretary of State for the Home Department
by Command of Her Majesty.
June 1999.

Cm 4368
£8.00

Foreword by The Home Secretary



Interception plays a crucial role in helping law enforcement agencies to combat criminal activity. On average, one in every two interception warrants which I issue results in the arrest of a person involved in serious crime. The proposals in this consultation paper will help to maintain it as the most powerful weapon in the armoury. And interception plays a wider role in the fight against terrorism of all kinds, and in the protection of the United Kingdom's vital national interest.

All interception of the public telephone system in this country takes place under a strict regime laid down by Parliament - principally the Interception of Communications Act 1985. But those who drafted the current legislation on interception of communications, some fifteen years ago, could not and did not foresee the extraordinary pace of change in the communications industry, especially in the past decade. Faced with a revolutionised communications industry and dated legislation on interception, sophisticated criminals and terrorists have been quick to put the new technology to use. The law must be revised if we are to preserve the ability of the law enforcement and intelligence agencies to prevent and detect serious crime and threats to our national security.

This revolution in communications technology is one of the imperatives for change in the law. But so too is the need to protect human rights - this has been uppermost in our minds in devising these proposals. Disproportionate, or unfettered, use of interception can have consequences for the rights of individuals.

There are some specific areas in which we need to improve the protection offered to the individual. There is currently no basis in law, for example, for the interception of communications on private telephone networks. We intend to put such interception on a statutory footing for the first time. This will ensure that the privacy of those who use these networks is respected, and that they have a means of redress if their communications are intercepted unlawfully.

Robust, independent safeguards are already in force. Interception may only take place when the information cannot reasonably be acquired by any other means. Each warrant is personally authorised by the relevant Secretary of State (in Scotland in respect of serious crime, authorisation will be given by the First Minister), and only when he or she is satisfied that it is strictly necessary. A senior judge reviews this process, and subjects the intercepting agencies to tough scrutiny. An independent tribunal investigates any complaints against the agencies. This document now proposes a new Code of Practice which will provide greater clarity about when and how applications for use of interception are authorised.

The Government is committed to building a safe, just and tolerant society. In the field of interception, there is a difficult balance to be struck. I believe our proposals strike the right balance and will be grateful for views on any of the proposals in this document.

JACK STRAW

INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM

Contents *Page*

Text of Articles 6, 8 and 13 of The European Convention on Human Rights

Article 6

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgement shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to the law.

3. Everyone charged with a criminal offence has the following minimum rights:

(a) to be informed promptly, in a language which he understands and in detail, of the nature and the cause of the accusation against him;

(b) to have adequate time and facilities for the preparation of his defence;

(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

(d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Article 8

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

2. 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.

Article 13

Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

Executive Summary

Background

In most developed countries, interception of communications is used by the law enforcement, security and intelligence agencies in their work against serious crime and threats to national security, including terrorism. The UK is no exception. Interception represents an indispensable means of gathering intelligence against the most sophisticated and ruthless criminals. Its value in the serious crime field is demonstrated by the fact that, in the years 1996 and 1997, lawful interception of communications played a part – often the crucial part – in operations by the police and HM Customs which led to:

- 1200 arrests;
- the seizure of nearly 3 tonnes of Class A drugs, and 112 tonnes of other drugs, with a combined street value of over £600 million;
- the seizure of over 450 firearms.

This Consultation Paper sets out the Government's proposals for reforming the legislation which governs the interception of communications in the United Kingdom. The proposed changes are designed to:

(a) update the legislation to take account of communications services introduced since the existing legislation was enacted

(b) extend the law to cover interception of private telephone networks

(c) provide a clear, statutory framework for authorising the disclosure of data held by communications service providers

(d) retain the existing safeguards which ensure that interception is authorised only when it is justified in relation to strict statutory criteria, and that the use of the power is subject to independent judicial oversight.

The Government intends to introduce legislation as soon as Parliamentary time allows, and invites views on the content of the legislation

Human Rights Act 1998

We recognise that, by its nature, interception of communications is a highly intrusive activity, affecting the privacy of the individual. The legal right to respect for a private and family life is established in Article 8 of the European Convention on Human Rights (ECHR), which is being incorporated into UK law in the Human Rights Act 1998. The ECHR recognises, however, that there are circumstances in a democratic society where it may be necessary for the state to interfere with this right, but only in accordance with the law and for certain clearly defined purposes. Where such interference does take place, Article 13 ECHR requires a means of redress to be available to the individual. The Government is committed to ensuring that interception of communications complies fully with the ECHR, and this paper describes the separate frameworks for authorisation, oversight and redress with which we propose to achieve this.

This paper deals only with interception of communications. The Government is aware that similar issues arise in relation to other forms of surveillance and the requirements of the ECHR. Many of these issues were addressed in the recent JUSTICE report "Under Surveillance"[1]. The Government is considering whether changes to current legislation should be extended to cover methods of intrusive surveillance other than interception of communications. Our conclusions will be announced in due course.

The law at present

The Interception of Communications Act 1985 (IOCA) placed interception of communications sent by post or by means of a public telecommunication system on a statutory basis for the first time. The main features of IOCA are summarised below:

(a) The Act created an offence of unlawful interception of communications by post or by means of a public telecommunication system.

(b) It established a framework controlling issue, renewal, modification and cancellation of warrants authorising interception of communications sent by post or by means of a public telecommunication system.

(c) It enshrined in law the principle that warrants may only be issued by the Secretary of State, and specified the purposes for which warrants may be issued as:

(i) in the interests of national security;

(ii) for the purpose of preventing or detecting serious crime; or

(iii) for the purpose of safeguarding the economic well-being of the United Kingdom.

(d) It placed strict safeguards on the extent to which intercepted material may be disclosed, copied and retained, requiring arrangements to be made to ensure that each of these is kept to a minimum.

(e) The Act established an independent oversight regime in the form of the Interception Commissioner, whose job is to keep under review the way in which the power to issue warrants is exercised and the operation of the safeguards described above.

(f) It set up a Tribunal to investigate complaints where the complainant believes that their communications have been intercepted in breach of the Act.

Why is there a need to change the law?

Since the 1985 Act was enacted there have been enormous changes in the telecommunications and postal market, and a great expansion in the nature and range of services available. For example:

- The number of telecommunications companies offering fixed line services has grown from two to around 150.
- Mobile telephones have developed from being virtually unheard of to the mass ownership which is seen today.
- The emergence of totally new services such as international simple resale, which offer cut price telephone calls abroad – there are currently over 200 of these.
- The satellite telephone market, while still in its infancy, will evolve rapidly in the next few years.

[1]Under Surveillance: Covert policing and human rights standards, published 1998.

- Communications via the Internet have grown dramatically in the last few years, and this part of the market continues to grow.
- The postal sector has also developed rapidly, with a huge growth in the number of companies offering parcel and document delivery services.

The legislation has not kept up with the changes in the communications marketplace; changes which criminals and terrorists have been quick to exploit for their own purposes. If we fail to bring the legislation up to date, we risk degrading the capability of the law enforcement, security and intelligence agencies ("the Agencies").

We also need to update our interception law to encompass private networks, which will ensure that the protection currently offered by IOCA to individuals using public telecommunications networks is extended to cover all networks. At present, there is no right of redress in UK law for an individual whose communications have been intercepted if the interception took place on the non-public side of the network. The proposed legislation will make this type of unauthorised interception unlawful, enabling us to give effect to the judgment of the European Court of Human Rights in the case of Halford v UK[2]. The law needs to recognise that there are perfectly respectable reasons for allowing employers to record telephone conversations in the work place; for example, in order to provide evidence of commercial transactions or to counter fraud. But the practice needs to be regulated by law, in a way which ensures that the rights of employees are respected in circumstances where they have a reasonable expectation of privacy. The legislation will provide a clear framework governing the interception of private networks, setting out the circumstances in which it may be authorised and the safeguards which should apply.

The Government believes that the law surrounding access to communications data is in need of revision. Itemised billing, for example, can be of tremendous investigative value, and it is right that in certain circumstances the authorities should be able to access this material. However, it also involves a measure of intrusion into individual privacy and it is essential that access should be carefully controlled in accordance with ECHR proportionality requirements, authorisation only being given where necessary and justified for clearly defined purposes. For these reasons we are proposing to establish a clear, statutory framework for access to communications data.

[2]EHRLR 551

SUMMARY OF LEGISLATIVE PROPOSALS

The broad areas in which change is proposed are as follows:

Existing Legislation	Proposed Changes
IOCA is restricted to interception of communications sent by post or by means of public telecommunication systems.	Interception legislation to encompass all communications in the course of their transmission by telecommunications operators or mail delivery systems.
Currently interception warrants specify the address[3] to be intercepted.	Interception warrants to specify a person, and to include a schedule listing all the addresses which the Agency wish to intercept in relation to that person[4].
Interception warrants may only be issued under the authority of the Secretary of State. Modifications may be made by Senior Civil Servants with the express authorisation of the Secretary of State, or by a person holding office under the Crown, where they have been expressly authorised by the warrant to do so.	The issue of the warrant to continue to be authorised by the Secretary of State[5]. Subsequent modifications to the warrant adding new addresses to be authorised at Senior Civil Service level. Provision to be made allowing urgent modifications with limited lifespan to be made by Head of Agency or nominated deputy who are expressly authorised by the warrant.
Interception warrants are served on the PTO or Post Office, who are required to intercept such communications as are described in the warrant.	Interception warrants to be served on the agency making the application, who will then use them to achieve the interception with reasonable assistance from the Communications Service Provider.
All warrants are authorised for an initial period of two months. Thereafter, warrants issued on serious crime grounds are renewed on a monthly basis and those issued on national security or economic well-being grounds are renewed on a six monthly basis.	All warrants to be authorised for an initial period of three months. Warrants to be renewed at three monthly periods (serious crime warrants) and six monthly (national security and economic well-being warrants), bringing them into line with intrusive surveillance[6] provisions.
There is currently no legislative framework for authorising interception of private (non-public) networks.	Interception on non-public networks to be brought within the scope of the legislation, requiring the Agencies to obtain a warrant before carrying out this type of interception.

[3]The term 'address' is defined in IOCA as meaning any postal or telecommunication address.

[4]It will remain possible to specify an address rather than a person where circumstances require.

[5]The duty of issuing IOCA warrants is normally undertaken by the Home Secretary, the Foreign Secretary, the Secretary of State for Scotland and the Secretary of State for Northern Ireland. From 1 July 1999, when the Scottish Parliament takes its powers, the power to issue IOCA warrants on serious crime grounds will pass to the First Minister.

[6]Provisions contained within Part III Police Act 1997 and Intelligence Services Act 1994.

Existing Legislation	Proposed Changes
There is no legislative framework which addresses recording or monitoring of communications in the course of lawful business practice.	Provision to be made allowing employers to continue recording communications in the course of lawful business practice to provide evidence of commercial transactions or any other business communication, in both the public and private sectors.
Communications data may be supplied voluntarily by holders for specified reasons (eg investigation of crime) under the Data Protection Act and the Telecommunications Act. They may additionally be required to produce it in obedience to a Production Order authorised by a Crown Court judge.	The law regarding provision of communications data for law enforcement, security or intelligence purposes to be amended to require the holder of such data to provide it in response to a properly authorised request.

The areas where no change is proposed

Along with the proposals for change which are contained in the above table and described in detail in this paper, there are several fundamental provisions contained within the Interception of Communications Act which have been unaffected by the developments outlined in the introduction and continue to work well. The Government proposes no change to these provisions, which are listed below:

- There will continue to be an offence of unlawful interception.
- There will be no change to the criteria which must be met before interception of communications may be authorised.
- There will be no change to warrantry procedures authorising interception of external communications.
- The strict safeguards regarding the extent to which intercept material is disclosed or copied will remain, continuing to limit this to the minimum necessary.
- There will continue to be a Tribunal to hear complaints.
- The Interception Commissioner will continue to oversee the use of interception.

CONSULTATION

The Government welcomes views on any matter relating to the proposals in this paper. Responses should be sent, by Friday 13 August 1999, to:

The Interception Legislation Team
Organised and International Crime Directorate
Room 735
Home Office
50, Queen Anne's Gate
LONDON SW1H 9AT

Responses may also be sent by e-mail to: ioca@homeoffice.gsi.gov.uk

The Government may be asked to publish responses to this Consultation Paper. Please let us know if you do not want your response to be published.

This document is available at www.homeoffice.gov.uk/

Part A – Interception and the Need for Change

Chapter 1
Interception Today

What is interception of communications?

1.1 Interception of communications occurs where a private communication between two or more parties, sent via a communications handling system, is covertly monitored in order to understand the content. It is not confined to any particular communications handling system; covert monitoring of private messages sent through telephone networks, e-mail systems, pager communications or other wireless transmissions are all examples of interception.

Why carry out interception and who does it?

1.2 There are massive potential profits to be made from crime (see box below). But with this potential gain, there is also the considerable risk of being arrested, prosecuted and convicted. It is hardly surprising, therefore, that with so much at stake, people involved in serious crime take precautions, both to protect their investment and minimise their chance of being caught. They are prepared to pay for the best advice and technology in order to reduce their risk as far as possible, leaving fewer weaknesses for the law enforcement agencies to exploit. Conventional investigation techniques do not work well against sophisticated criminals who know how to counter them, and it is therefore necessary for the law enforcement agencies to concentrate on the remaining weaknesses in the structures of an organised crime group. One of these is their communications.

> Heroin, a class A drug, may be bought in bulk in Pakistan at £850 per kilo, and sold in the UK for around £24,000. At street level the price is around £74 / gramme[7]. The potential profits are enormous, but so are the penalties. Upon conviction, a smuggler of 1 kg of a class A drug could expect to receive a prison sentence of around 10 years[8].

1.3 It is virtually impossible to organise a complex crime without communicating over public networks, and this is particularly true where there is an international dimension, as is increasingly the case. Interception can exploit this weakness in the criminal structure, providing the Agencies with an opportunity to gather intelligence on crimes as they are being planned and providing an invaluable insight into the thoughts and intentions of the criminals. Accurate intelligence enables operations to be mounted with a far greater chance of success than may otherwise occur. In March 1981 Lord Diplock, the forerunner of the present day IOCA Commissioner, made a comment in his Report to the Prime Minister which remains equally valid today:

> "the interception of communications, particularly telephone conversations, remains an effective, indeed an essential, weapon in the armoury of those authorities responsible for the maintenance of law and order and the safety of the realm. Major crime has become more highly organised, international trafficking in drugs brings enormous profits, and terrorism has become a world wide problem; and all this has made it more necessary for the members of criminal gangs in each of these categories to communicate with one another by telephone about their activities and plans."

[7]December 1998 UK average figure.

[8]Sentencing guidelines laid down by the Court of Appeal in R v Aramah (1983) and revisited in R v Aranguren (1994).

1.4 Warrants for interception are obtained on application by the National Criminal Intelligence Service, Metropolitan Police Special Branch, HM Customs and Excise, Royal Ulster Constabulary, Scottish Police Forces, the Security Service, the Secret Intelligence Service and the Government Communications Headquarters.

1.5 In 1998, 2031 interception warrants were authorised by the Home Secretary and the Secretary of State for Scotland (from 1 July 1999, when the Scottish Parliament takes its powers, serious crime warrants in Scotland will be issued by the Scottish First Minister), of which 487 were in force on 31 December 1998. It is clear from these figures that no more than a tiny fraction of all communications are intercepted, and that this form of investigation is reserved for only the most serious cases.

> Serious crime is defined in section 10(3) of the Act as an offence involving the use of violence or resulting in substantial financial gain or involving a large number of persons in pursuit of a common purpose, or alternatively as an offence for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more. All of the serious crime warrants which I have examined have been concerned with offences which would rank as serious crime by any reckoning. Nearly all of them have fallen within the first part of section 10(3). All have comfortably passed the three years imprisonment test in the second part of the subsection.
>
> *Extract from the Report of the Commissioner for 1997*

How is interception currently regulated?

1.6 With certain narrow exceptions, it is unlawful to intercept a communication on a public telecommunication system except under warrant issued on the personal authority of the Secretary of State. The Secretary of State may issue a warrant only where he is satisfied that it is necessary:

(a) in the interests of national security;

(b) for the purpose of preventing or detecting serious crime; or

(c) for the purpose of safeguarding the economic well-being of the United Kingdom.

He must also consider whether the information sought is necessary or could reasonably be acquired by other means.

1.7 Warrants last for two months. They may be renewed, but only, again, on the personal authority of the Secretary of State who must be persuaded that the criteria for authorisation are still valid. Upon renewal, warrants issued on serious crime grounds last for one month, and warrants issued on national security or economic well-being grounds last for six months.

Safeguards

1.8 The Interception of Communications Act provides for the appointment, by the Prime Minister, of a Commissioner. The Commissioner is a person who holds or has held high judicial office and is independent of Government and of the intercepting Agencies. The present Commissioner is the Rt Hon the Lord Nolan of Brasted. His function it is to oversee the exercise of the Secretary of State's power to issue warrants. In order to do this he undertakes inspections of the intercepting Agencies and relevant Government Departments to ensure that they are complying with the Act. The Commissioner is given full access to all relevant papers and he selects warrants for inspection, reviews files and associated documentation, and discusses cases directly with operational staff. He makes a written report annually to the Prime Minister which is laid before Parliament, although provision is made allowing certain sensitive matters to be withheld by the Prime Minister if he feels it necessary.

1.9 There is also a statutory Tribunal to which members of the public may apply if they believe that there has been any contravention of the warrant-issuing provisions in the Act. This Tribunal, which comprises five senior members of the legal profession is independent of the intercepting Agencies and Government. They have right of access to all relevant material held by the Agencies and may, if necessary, call upon the Commissioner for assistance to investigate complaints. If the Tribunal concludes that there has been a contravention of the Act it must inform the applicant, report its findings to the Prime Minister and, if it thinks fit, make an order which may quash the interception warrant, require the destruction of intercepted material, and / or require the Secretary of State to pay compensation.

Since the Tribunal was established in 1986 it has considered 568 complaints. 5 further cases were under consideration on 31 December 1997. It is a published fact (as set out in the Annual reports) that the Tribunal has never found there to have been a contravention of the provisions of the Act. This has led to a measure of suspicion as to the effectiveness of the Tribunal's work. The fact is that investigation by the Tribunal has revealed that in only 8 of the 568 cases was interception being carried out by a Government agency; and in each of those 8 cases the interception was authorised by a valid warrant issued by the Secretary of State. In these circumstances it is hardly surprising that no contravention of the Act by Government Agencies has been found to exist.

Extract from the 1997 Report of the Commissioner

Chapter 2

The History of Interception in the United Kingdom

Before 1937

2.1 The first public reference to the warrant of the Secretary of State authorising the opening of letters is the Proclamation of May 25th, 1663. Interception of telephone communications occurred without warrant prior to 1937, at which point this policy was reviewed by the Home Secretary and the Postmaster-General and it was decided that interception of telephones could only occur in future on the authority of a warrant signed by the Secretary of State.

The 1951 Guidelines

2.2 In September 1951 the Home Office issued guidelines to the Metropolitan Police and Customs and Excise which laid out the conditions which must be satisfied before a warrant for interception of communications could be authorised by the Secretary of State. They were:

(a) The offence must be really serious;

(b) Normal methods of investigation must have been tried and failed, or must, by the nature of things, be unlikely to succeed if tried;

(c) There must be good reason to think that an interception would result in a conviction.

The Home Office explained in a letter to the police that 'serious crime' offences were offences for which a man with no previous record could reasonably be expected to be sentenced to three years' imprisonment, or offences of lesser gravity in which a large number of people were involved. A separate letter to Customs defined 'serious crime' as 'involving a substantial and continuing fraud which would seriously damage the revenue or the economy of the country if it went unchecked'.

The Birkett Report[9]

2.3 This report was the result of an inquiry into the interception of communications by the Committee of Privy Councillors. It provides an account of the grounds upon which an application for a warrant could be made at that time.

The report stated the principles governing the issue of warrants to the Security Service as follows:

(a) There must be a major subversive or espionage activity that is likely to injure the national interest;

(b) The material likely to be obtained by interception must be of direct use in compiling the information that is necessary to the Security Service in carrying out the tasks laid upon it by the State; and

(c) Normal methods of investigation must have been tried and failed, or must, by the nature of things, be unlikely to succeed if tried.

Less stress was laid upon the need for the Security Service to secure convictions, due to the nature of its duties in safeguarding the State.

[9]Cmnd 283, published October 1957.

The 1980 White Paper[10]

2.4 This White Paper brought up to date the account of interception of communications given in the Birkett Report. It confirmed that interception may be undertaken only with the authority of the Secretary of State given by a warrant under his own hand. It also listed the conditions which must be satisfied for the police, Customs and Excise or the Security Service to apply for a warrant, which were very similar to those in the Birkett Report.

2.5 In a statement to Parliament introducing the 1980 White Paper[11] the then Home Secretary explained that the Government had decided not to introduce legislation on these [interception] matters, but that it would be desirable if there were a continuous independent check that interception was being carried out in accordance with the established purposes and procedures.

The Diplock Report[12]

2.6 In order to carry out the 'continuous independent check' referred to above, Lord Diplock was appointed, and his first Report was published in March 1981. His terms of reference were:

> "To review on a continuing basis the purposes, procedures, conditions and safeguards governing the interception of communications on behalf of the police, HM Customs and Excise, and the Security Service as set out in Cmnd 7873; and to report to the Prime Minister."

2.7 While conducting his review of current interception of communications practices Lord Diplock considered whether the practices were effective to ensure that the following six conditions were observed:

(a) that the public interest which will be served by obtaining the information which it is hoped will result from the interception of communications is of sufficient importance to justify this step;

(b) that the interception applied for offers a reasonable prospect of providing the information sought;

(c) that other methods of obtaining it such as surveillance or the use of informants have been tried and failed or from the nature of the case are not feasible;

(d) that the interception stops as soon as it has ceased to provide information of the kind sought or it has become apparent that it is unlikely to provide it;

(e) that all products of interception not directly relevant to the purpose for which the warrant was granted are speedily destroyed; and

(f) that such material as is directly relevant to that purpose is given no wider circulation than is essential for carrying it out.

I conclude, therefore, from the monitoring of the procedures for the interception of communications that I have been able to undertake up to the present date, that those procedures are working satisfactorily and with the minimum interference with the individual's rights of privacy in the interests of the public weal. I propose to continue to follow the system described in this Report of random checks of applications for issue of warrants on behalf of each of the applicant authorities.

Extract from The Diplock Report

[10]Cmnd. 7873 'The Interception of Communications in Great Britain', published April 1980.

[11]Hansard, 1 April 1980, column 205.

[12]Cmnd 8191 'The Interception of Communications in Great Britain', published March 1981.

The 1985 White Paper[13]

2.8 The above White Paper indicated the Government's intention to introduce legislation on the interception of communications. The need for legislation had become apparent as a result of a European Court of Human Rights judgment (the Malone case). In this, while the Court acknowledged that detailed procedures existed governing the interception of communications, and that interception under these procedures was lawful under English law, it concluded that the law did not indicate with reasonable clarity the scope and manner of exercise of the discretion conferred on the public authorities. The Government's aim in introducing legislation was "to provide a clear statutory framework within which the interception of communications on public systems will be authorised and controlled in a manner commanding public confidence".

2.9 The White Paper described the proposals for statutory frameworks covering authorisation of interception, use and storage of intercept material, independent oversight of the warrantry process by a Commissioner, and a complaints procedure to be carried out by an independent Tribunal. It concluded by stating "As the European Court of Human Rights has recognised, a balance must be sought between the individual's right to the privacy of his communications and the need for a properly regulated system of interception in order to protect democratic society as a whole. The Government considers that the proposals set out in the preceding paragraphs achieve this balance, as regards both the legislation and the conditions and procedures which will apply to its operation".

The Interception of Communications Act 1985

2.10 The 1985 White Paper was followed by the Interception of Communications Act 1985 (IOCA) which incorporated all of the statutory frameworks described in para 2.9. Challenges to IOCA have been successfully defended in Strasbourg, which is perhaps an indication of how robust this legislation has been. Some of the recent cases are outlined below:

- *Campbell Christie v United Kingdom*: decision 27 June 1994. Applicant was General Secretary of the Scottish Trades Union Congress. The case concerned the alleged interception by GCHQ of telexes to the applicant from East European trade unions. Scope and manner of the exercise of powers to intercept communications and make use of the information obtained were indicated with the required degree of certainty to be "in accordance with the law". Commission followed the earlier cases of Esbester and Hewitt and Harman to approve the role of the Tribunal and Commissioner under the 1985 Act.
- *Matthews v United Kingdom*: decision 16 October 1996. Applicant was a peace campaigner. During civil action against the Ministry of Defence, she complained of interception of her telephone. So far as lawful interception was concerned, the Commission saw no reason to depart from its findings in Christie. They found no evidence of unlawful interception.
- *Preston v United Kingdom*: decision 2 July 1997. Principally an Article 6 case. Interception material was destroyed pursuant to section 6 of IOCA. The Commission accepted the submission of the United Kingdom that the effect of section 9 of IOCA is to place the prosecution and the defence on an equal footing, meaning that there was no inequality of arms. On Article 8, the Commission again endorsed the Campbell Christie decision.

2.11 IOCA put interception of communications onto a statutory footing for the first time, clearly setting out the reasons for which an interception warrant may be issued, the procedures for authorisation of warrants, safeguards mechanisms, oversight arrangements and complaints procedures.

[13]Cmnd. 9438 'The Interception of Communications in the United Kingdom', published February 1985.

Chapter 3

The Need for New Legislation

Interception and public safety

3.1 The effect of section 2(3) IOCA is that even if the application for interception fits one of the criteria (e.g. for the purpose of preventing or detecting serious crime), the Secretary of State is still required to consider whether the information sought is necessary or could reasonably be acquired by other means before issuing a warrant.

3.2 This means that not only is the use of interception reserved for use against only the most serious criminals and terrorists, it is also a method of last resort. In many cases it would not be possible to mount successful operations against these types of targets without the use of interception, meaning that the crimes being planned would go ahead.

3.3 This clearly has consequences for public safety. Prevention of a terrorist act removes the threat to public safety posed by the planned action. The same holds true for serious crime posing a threat to the public such as armed robbery or kidnapping. But it is also important to consider the consequential effects of serious crime. Taking drug trafficking as an example, this extract taken from the Report of the UK Anti-Drugs Co-ordinator[14] shows the knock on effect upon the public of the drugs trade:

- Many police forces estimate that around half of all recorded crime has some drug related element to it, whether in terms of individual consumption or supply of drugs, or the consequent impact of it on criminal behaviour.
- A small number of people are responsible for huge numbers of crimes - 664 addicts surveyed committed 70,000 offences over a three month period.
- Latest indications from a random sample of suspected offenders arrested by the police suggest that over 60% of arrestees have traces of illegal drugs in their urine.

Developments in technology and services

3.4 IOCA had the aim of providing a clear statutory framework within which the interception of communications on public systems would be authorised and controlled in a manner commanding public confidence. The way in which the scope of the Act was defined was through use of definitions taken from the Telecommunications Act 1984 for communications by telephone and the Post Office Act 1969 for communications by post. Use of these definitions means that IOCA warrants may only be served on persons licensed as a Public Telecommunication Operator[15] (PTO) or on the Post Office. When IOCA was enacted this meant that all communication services available to the public fell within these definitions, because they were carried on either the public telecommunication system or via Royal Mail.

[14]Cm 3945, 'Tackling Drugs to Build a Better Britain', published April 1998.

[15]Defined in section 9(3) Telecommunications Act 1984.

3.5 A number of services have been developed since IOCA was introduced which are not licensed as PTO services, yet are nevertheless telecommunication services to the public. These include International Simple Resale (ISR)[16], some 'value added' services such as voicemail, and e-mail services through Internet Service Providers (ISPs), which are covered in more detail below. Radio pagers have developed from being a simple beeper into a means of sending whole messages, yet pager service providers, too, fall outside IOCA.

3.6 It is clear, therefore, that the current statutory framework for interception of communications does not achieve its original purpose, and in any event it needs to be extended to cover areas which were not addressed by the Act.

E-mail

3.7 Although IOCA is not specific about the type of traffic which may be lawfully intercepted under a warrant, the Act does restrict any such interception to public networks. E-mail which does not pass through a PTO's system therefore cannot lawfully be intercepted, while interception of e-mail which does pass through a PTO's network would normally be more efficiently intercepted at the ISP rather than on the network itself. Furthermore, the present system leads to inconsistency in that the e-mail carried on the network of a PTO which is also an ISP can lawfully be intercepted on the ISP system, while e-mail on the system of an ISP which is not licensed as a PTO can only be intercepted on the PTO network carrying the calls, if at all.

Private networks

3.8 Under the 1985 Act there is no statutory framework for interception on non-public telecommunications networks. Such networks include hotel and workplace systems. This means that, currently, it is possible for communications to be intercepted on the non-public part of a telecommunication system without an offence being committed in UK law and without any need for statutory authorisation. In the case of Halford v UK in the European Court of Human Rights (ECtHR) this deficiency became apparent because Article 8 of the Convention only allows public authorities to interfere with a person's privacy 'in accordance with the law'. The Court ruled that because UK law relating to interception does not extend to non-public telephone networks, this form of interception cannot be carried out in accordance with the law and there is no effective remedy. New legislation will be an opportunity to address this deficiency and extend the protection against unlawful interception provided by IOCA. Other cases which have highlighted inadequacies in the UK's interception legislation are:

- *R v Effik*: decision 21 July 1994[17]. A cordless telephone operated through a base unit which is connected to the public telecommunications system is not part of that public system but is instead a private system connected to the public system. Accordingly, the interception by the police of telephone conversations on a cordless telephone is not subject to the Interception of Communications Act 1985 and evidence at a criminal trial of such conversations is not rendered inadmissible under s9(1) of the Act by reason of the fact that the interception has taken place without a warrant.
- *R v Ahmed and others*: decision 29 March 1994. The interception of a communication takes place when, and at the point where, the electrical impulse or signal which is passing along the telephone line is intercepted in fact. If there is an interception of the private system, the communication which is intercepted is not at that time passing through the public system.

[16]ISR companies buy bulk international line space from PTOs and resell the calls, undercutting the PTO pricing.

[17]Crim LR 832, 99 Cr App Rep 312, 158 JP 749.

Monitoring for business purposes

3.9 There are a number of legitimate reasons why non-public network operators might wish to monitor or record communications passing over their network. Some, particularly within the financial sector, use recording as a tool to provide evidence of transactions. Some operators offering telesales services monitor their staff when they are dealing with customers by telephone for training and development or quality control purposes. And some employers need to monitor communications for internal security or the prevention of fraud. There is a need to take account of this requirement in new legislation, yet also to protect the rights of the employee against interception where they have a legitimate expectation of privacy.

Wireless Telegraphy

3.10 The Wireless Telegraphy Act 1949 provides a legal framework for interception of communications sent by wireless telegraphy but does not have the same rigorous authorisation, oversight and complaints mechanisms as are provided by IOCA. As means of communication increasingly make use of both telecommunications and wireless telegraphy networks, it is logical that any interception of communications, regardless of the physical point at which it occurs, should be treated the same way in law.

Postal Communications

3.11 In the field of postal communications, only letters and parcels carried by the Post Office may be intercepted under an IOCA warrant. While mail is intercepted far less frequently than telephones[18], criminals are still forced to use the mail and interception of their post can provide vital intelligence. The Act does not allow a warrant to be served upon providers of courier or parcel delivery services, yet the rapid growth of such services now means that a large percentage of mail other than letters is not carried by the Post Office.

Provision Of Communications Data

3.12 Communications data is information held by communication service providers relating to the communications made by their customers. This includes data such as itemised billing, routing information and subscriber details.

3.13 As has been explained earlier in this paper, everyone needs to communicate in order to arrange their day to day activities, and criminals are no exception. Their need to communicate during the planning and execution of crime is a weakness which the authorities exploit, often with considerable success. Telephone itemised billing, for example, provides a great deal of information on individuals' contacts and how they organise their life. This can be used in the planning of operations, the gathering of intelligence and, ultimately, it regularly assists in the prosecution of criminals.

3.14 Provision of communications data by telecommunications operators is currently authorised by a variety of statutes. Both s45 Telecommunications Act 1984 (as amended by IOCA) and s28 Data Protection Act 1984 (soon to be replaced by the 1998 Act) allow holders of such data to provide it voluntarily for specific purposes, including the prevention or detection of crime, the purposes of criminal proceedings and in the interests of national security. In addition a holder of communications data may be required to produce it in obedience to a Production Order, which can be applied for under a variety of statutes and is authorised by a Crown Court judge.

[18]In 1998 a total of 118 postal IOCA warrants were issued by the Home Secretary and Secretary of State for Scotland.

Part B – The Government's Proposals

Chapter 4
Scope

A single legal framework

4.1 The intention is to provide a single legal framework which deals with all interception of communications in the United Kingdom, regardless of the means of communication, how it is licensed or at which point on the route of the communication it is intercepted. This means that the scope of the Bill will be wider than that of the Interception of Communications Act 1985 (IOCA) in three specific areas; non-public networks, wireless telegraphy and interception of mail.

4.2 In order to implement the Halford judgment we propose to extend the interception regime to all telecommunications networks, regardless of whether they are licensed as public or not. This will of course include Public Telecommunication Operators which currently fall within the scope of IOCA, but also Internet Service Providers and International Simple Resale Operators. It will also cover interception of business telecommunication services, ranging from basic networks of a few lines found within a small office to large networks linking offices, in both the public and private sectors.

4.3 We propose that communications carried wholly or partly by wireless telegraphy should be included within the scope of the interception regime, requiring the Agencies to seek a warrant where interception of wireless telegraphy would interfere with the privacy of the communicating parties.

4.4 It is also proposed that the interception regime will encompass all mail handling and delivery systems, which include all parcel and courier services in addition to the Royal Mail and Parcel Force.

4.5 The Government believes that it should not make any difference how a communication is sent, whether by a public or non-public telecommunication or mail system, by wireless telegraphy or any other communication system. Nor should the form of the communication make any difference; all interception which would breach Article 8 rights, whether by telephone, fax, e-mail or letter, should all be treated the same way in law. A single authorising framework for all forms of lawful interception of communications will mean that each application will follow the same laid down procedure and will be judged against a single set of criteria. This will ensure that this type of intrusive activity is used only when justified, necessary and, in the case of criminal investigations, proportional to the offence.

4.6 It is not proposed that the warranted interception regime will affect recording or monitoring of communications where this is done in the course of lawful business practice and where the system operator has taken reasonable steps to inform parties to the communication that it may occur. Specific authorisation, granted on a case by case basis, to carry out interception on non-public networks is only required where the activity occurs in secrecy. System operators carrying out overt recording or monitoring are already bound by a 'Privacy of Messages' condition within their operating licence which requires them to "make every reasonable effort to inform parties to whom or by whom a Live Speech Telephone Call is transmitted before recording, silent monitoring or intrusion into such Call has begun that the Live Speech Telephone Call is to be or may be recorded, silently monitored or intruded into". It is quite common to see a warning of this type included in advertising, with the aim of informing members of the public who may choose to use the service being advertised.

The Government invites comment on the scope of communication services which should be subject to interception legislation.

Chapter 5

Communication Service Providers

Effects Upon Communication Service Providers[19]

5.1 The Interception of Communications Act currently requires the person to whom a warrant is addressed to intercept, in the course of their transmission by post or by means of a public telecommunication system, such communications as are described in the warrant. This has required public telecommunication operators and the Post Office to design their communications systems to be able to comply with interception warrants. Since, at present, Communication Service Providers (CSPs) which do not fall within the scope of IOCA cannot be served with an interception warrant, there is no requirement for them to have any intercept capability.

5.2 As a result of the increase in scope of the Bill, the intercepting agencies will approach some CSPs for the first time in order to execute interception warrants (e.g. Internet Service Providers). There will be two specific areas in which all communication service providers will be required to provide assistance, although the level of this requirement will vary depending upon various factors.

Provision of reasonable intercept capability and assistance

5.3 Communication Service Providers will be required to take reasonable steps to ensure that their system is capable of being intercepted. This will be an ongoing requirement which CSPs will have to consider each time they develop their network or introduce new services. CSPs will also be required to provide reasonable assistance to effect warranted intercepts. The requirement currently contained within IOCA[20] does not take account of a PTO's ability to comply with the terms of an interception warrant, but with the increase of the scope of the interception regime the Government believes that it is now necessary to recognise that some CSPs may have difficulty complying with such a requirement. One reason for this is because there are so many CSPs of varying size and technical ability, and a large CSP with substantial technical resources may find it much easier to provide assistance than a smaller one with more limited assets. We believe that by introducing a requirement for CSPs to provide reasonable assistance, this will allow a sensible level of co-operation to be developed between individual service providers and the intercepting agencies.

5.4 While the Government recognises that this will represent new formal obligations on CSPs which were not previously included within the scope of the 1985 Act, in practice the same requirements have been met by PTOs since IOCA came into force. It is important that there is a level commercial playing field for all CSPs within the UK and that requirements imposed by the Government should not place any one section of the UK's communication industry at a disadvantage when operating internationally. Maintenance of an interception capability forms a

[19]The term Communication Service Provider (CSP) is used to describe any person providing publicly available communication services or authorised to provide telecommunication systems or networks for the conveyance of publicly available telecommunication services.

[20]S2(1) IOCA……the Secretary of State may issue a warrant requiring the person to whom it is addressed to intercept, in the course of their transmission by post or by means of a public telecommunication system, such communications as are described in the warrant; and such a warrant shall also require the person to whom it is addressed to disclose the intercepted material to such persons and in such a manner as are described in the warrant.

basic requirement for providers of communication services in countries where these service providers are in commercial competition with the UK, both in Europe and globally, including countries such as France, Germany, the Netherlands, Sweden, Canada, the USA and Australia. We therefore feel that, viewed in an international context, the proposed requirements are not unreasonable nor will they place the UK's communication services at a commercial disadvantage.

Who decides what is reasonable?

5.5 The Government proposes that the Secretary of State should decide what level of assistance is reasonable in respect of each CSP. In order to ensure that the requirements are proportionate and fair, it will be important to take into account such factors as the resources available to the company; the likely demand for interception from the Agencies; and the technical complexity of providing an interception capability. Although the diversity of the communications market will make it impossible to impose uniform requirements upon all CSPs, the Government will seek to ensure, as far as possible, that broadly equivalent requirements are placed upon companies competing in the same market sector.

5.6 In reaching a decision on what constitutes appropriate requirements to meet the Agencies' needs, the Secretary of State will take full account of internationally recognised standards such as the International User Requirements for the Lawful Interception of Communications[21] and other interception standards (e.g. those produced by the European Telecommunications Standards Institute). The Government also proposes to appoint an independent body to provide impartial advice on how to balance the requirements of the Agencies and CSPs. This should help to ensure that any requirements are reasonable, proportionate and do not place CSPs at a disadvantage compared with their competitors. The Government is at present inclined to ask OFTEL to perform this function.

Cost implications and international comparisons

5.7 In accordance with the existing practice for warrants under IOCA, the Government will expect Communication Service Providers to pay for the provision and maintenance of the basic intercept capability defined in the requirements issued by the Secretary of State. However, the Government will meet the marginal costs incurred by CSPs (i.e. the costs associated with implementing individual interception warrants), as occurs under existing arrangements with PTOs.

5.8 It is important to recognise that these proposals are consistent with existing legislation and practice in many other countries. For example, similar requirements already apply to Communication Service Providers elsewhere in the European Union including France, Germany, the Netherlands and Sweden, and in a number of non-EU countries (e.g. the USA, Canada and Australia). The Government will, however, endeavour to minimise any additional burdens on industry, particularly during the transitional period prior to the entry into force of the new legislation.

The Government recognises that these obligations will be of interest to industry and would welcome views on the issues set out in this section. In order to assess the cost and impact of the above proposals, we have included a number of specific questions at the end of this document, to which replies from providers of communication services are invited.

[21]The International User Requirements were adopted by Member States of the European Union in the Council Resolution of January 1995, and have subsequently been adopted by the Governments of the USA, Canada, Australia and New Zealand.

Chapter 6

International Developments

International Co-operation on Interception of Telecommunications

6.1 Recent developments in the telecommunications market have made it increasingly difficult for law enforcement agencies in the European Union and elsewhere to maintain existing interception capabilities. In particular, there may be circumstances where it is necessary to seek the assistance of another country in order to intercept the telecommunications of a person on UK territory. Existing mutual legal assistance arrangements are also used by most Member States of the European Union for the purpose of intercepting the communications of persons on the territory of other Member States. However, at present the UK does not comply with requests to intercept persons on UK territory.

6.2 A draft Convention on Mutual Legal Assistance is currently under negotiation in the European Union with the aim of providing a specific legal framework for mutual assistance on interception matters. The draft Convention deals with a wide range of scenarios. In particular, it would provide a legal basis for:

- Seeking technical assistance to implement an interception warrant against a person on the territory of the intercepting Member State; and
- Seeking the co-operation of another Member State to intercept a person on its territory.

In the first case, the draft Convention would place the requested Member State under an obligation to provide assistance where it is satisfied that a valid interception warrant has been issued by the requesting Member State.

In the second case, the requirements of national law would apply to both the requesting and requested Member State. In effect, this would establish a double-lock of safeguards. This means that the UK would not agree to requests by other Member States to intercept targets on UK territory unless the Secretary of State were able to issue a warrant in accordance with the criteria and safeguards in UK national law. The UK would also be able to impose conditions on the use of intercept material by other Member States, provided that these conditions would be imposed in domestic cases.

6.3 If agreed, the Convention will require changes to the UK's interception legislation in order to allow the UK to co-operate with other Member States. The latest text of the Convention is currently under consideration by the Parliamentary Scrutiny Committees.

Chapter 7

Warrantry Procedures

Authority to intercept

7.1 The law currently requires interception to be personally authorised by the Secretary of State. This is done by the facts of the case being presented to the Secretary of State who considers whether the use of interception is justified. If he or she decides that it is, they sign the warrant which authorises interception to be carried out. The warrant is then served upon the PTO or Post Office. In an emergency, it is possible for a warrant to be issued by a senior civil servant, but only after the Secretary of State has been briefed on the case and has given his or her specific authority.

7.2 Other authorisation frameworks have been examined during the review of IOCA, including judicial warranting or a system based upon the model of the Police Act 1997. While both would have advantages, particularly in their ability to meet the operational needs of the Agencies, there would remain the need for the Executive to issue warrants applied for on national security or economic well-being grounds, perhaps leading to parallel warranting arrangements.

7.3 The alternative options have been carefully considered and compared with the existing Secretary of State warranting procedures. On balance, the Government is not persuaded of the need to depart from the current means of authorising interception of communications and proposes to continue with the long established principle of Secretary of State authorisation.

Format of Warrant

7.4 The law requires interception warrants to specify a telephone number or a postal address, which is a way of identifying the communications to be intercepted. This approach worked well in 1985 because people did not normally have access to multiple means of communication, nor could they easily change from one PTO to another. For these reasons there was often only a single warrant per person being intercepted and the need to cancel the warrant and issue a new one in respect of the same person arose infrequently.

7.5 Advances in technology and the growth of the communications market now mean that one person can easily have access to many different types of communication, and it is relatively simple to change any one of them. This often leads to a number of warrants being issued in respect of one person, because his communication services are provided by several different PTOs. Each of these warrants, despite the fact that they are sought against the same person on the same grounds, must be applied for separately by the intercepting Agency and each must be authorised individually by the Secretary of State. This duplication of effort occurs not just at the time of warrant issue, but also each time an application is made to renew the warrant. Furthermore, a simple change in telephone number by the person being intercepted requires a fresh application to be made to the Secretary of State for the new number, and corresponding cancellation or modification of the existing warrant to remove the old one.

7.6 For these reasons the Government believes it is no longer practical to issue a separate warrant to each operator providing telecommunications or postal services to the same person, and proposes that these arrangements should be replaced by a single warrant authorising interception of all specified communications addresses relating to the person named on the face of it. The way this will work in practice is as follows:

(a) The warrant application will comprise the background to the case and a justification of the grounds upon which interception is sought, as it does at present. It will also specify each of the communications addresses which the person is believed to be using, and the reasons why the Agency considers it necessary to intercept each of them. Attached to this document will be the warrant itself and a schedule listing each of the communications addresses described in the application.

(b) If the application is approved, the Secretary of State will sign the warrant, which will give authority for each of the communications addresses listed in the schedule to be intercepted.

(c) The schedule, but not the warrant, may be modified subsequently by senior officials (see paragraph 7.8 below).

7.7 In this way the Secretary of State will not be authorising interception of individual communications addresses, but instead certifying that the facts of the case meet the criteria upon which interception may be authorised, and that the person specified within the warrant is a person upon whom interception is justified.

Modification of Warrants

7.8 IOCA allows interception warrants to be modified to include a new number by the Secretary of State or, in an urgent case, by a person expressly authorised by the Secretary of State. Such a modification is required when a person being intercepted changes the communications address listed or acquires a new one[22]. Under the current legislation, every time this occurs the interception warrant must go back to the Secretary of State for modification. The ability of criminals to change their phones quickly places an undue burden on the process and threatens to undermine its effectiveness.

7.9 While it is clearly right that each case should be carefully checked to ensure that the correct telephone numbers or addresses are being intercepted and that the case linking each number or address with the target of interception is properly made, the Government does not believe that this should require the same level of authority as is necessary for the issue of an original warrant. Where the Secretary of State has given authority for interception to take place against a person for specified purposes, modification of warrants should be carried out on the Secretary of State's behalf by senior officials in a warrant issuing department.

7.10 On occasion it is necessary to make an urgent modification to a warrant, for instance during a crucial phase of an operation when a target of interception changes their telephone. IOCA currently allows for this, providing a means for an official to make the modification where they have been expressly authorised by the warrant to modify it on the Secretary of State's behalf. Modifications made in this way have a limited lifespan[23].

[22]Because IOCA warrants are addressed to a specific PTO, modification is only possible where the person being intercepted changes a communications address but stays with the same PTO. Where this is not so, the Agency must apply for a new IOCA warrant.

[23]S 5(5) IOCA. Modifications made in this way last for five working days following the day of issue.

7.11 Where there is an urgent need to modify a warrant the Government proposes that the modification will be authorised at Director General or nominated deputy level within each intercepting agency, providing they were expressly authorised by the warrant to modify it on the Secretary of State's behalf. We propose that modifications made in this way will have the same five day limited lifespan.

Duration of Warrants

7.12 Currently, all new warrants authorised by the Secretary of State are valid for two months. Upon renewal, warrants applied for on national security or economic well-being grounds are valid for six months, serious crime warrants are valid for one month. The increasing length and complexity of operations, particularly serious crime operations, means that both these periods are simply too short. Particularly during the planning stages of a crime, it is quite normal for the investigation to progress quite slowly. This means that the Secretary of State is required to renew very large numbers of warrants on a monthly basis, often without a substantially altered intelligence background, with the consequence that there is little or no value added to the oversight procedure.

7.13 It is proposed that all warrants are valid for an initial period of three months and that upon renewal, a serious crime warrant will remain valid for three months. This would be in line with the Police Act provisions. National security and economic well-being warrants will continue to be valid for six months on renewal. As is the case now, the renewal period of all warrants is unaffected by any modifications which occur between renewals.

Cancellation of Warrants

7.14 Under the current system, once an intercepting agency no longer requires an intercept or can no longer justify the intercept on the grounds for which the warrant was issued, the intercept is immediately suspended. At this point the communication, to or from the subject of the warrant, is no longer being intercepted. The warrant is then sent for cancellation, which is carried out by the Secretary of State or officials acting on his behalf.

7.15 No changes are proposed to this procedure. It is rare for the Secretary of State himself to cancel warrants, the procedure normally being delegated to the persons acting on behalf of the Secretary of State. However, since the Secretary of State retains overall responsibility for interception and authorises each warrant at its outset it is proper that he should also retain the power to cancel warrants.

Code Of Practice

7.16 These proposals for interception legislation will be underpinned by a Code of Practice which will provide greater clarity regarding the circumstances in which an application for use of interception may be made and the processes and required authorisation levels surrounding all aspects of interception warranting. The Code will lay down the special procedures to be followed if it is necessary to intercept material which falls into a particularly sensitive category, such as legally privileged or other material of a similarly sensitive nature. The Government plans to hold a separate consultation exercise on the proposals for the Code of Practice.

Chapter 8

Use of Intercept Material in Evidence

8.1 Section 9 of the Interception of Communications Act 1985 has the effect of prohibiting the evidential use of intercept material gathered under a warrant issued under the Act. The value of this provision has been the subject of much debate over the years, with opinions sharply divided. More recently, the use of foreign intercept material in UK trials has highlighted the difference between our practice and that of Europe.

8.2 There are strong arguments both for the repeal and retention of this particular part of IOCA. Those seeking repeal believe use of this material is one of the few ways of gathering evidence against those who plan crimes but engage others to carry them out. The Inquiry into Legislation Against Terrorism, undertaken by Lord Lloyd[24] addressed the law on interception evidence, recommending that "section 9 of IOCA be amended so as to allow the prosecution to adduce intercept material in cases affecting national security….".

8.3 The main counter-argument, for retention of the prohibition on evidential use, is that exposure of interception capabilities will educate criminals and terrorists who will then use greater counter interception measures than they presently do. This would mean that any advantage gained by repeal would be short lived and would make interception operations more difficult in the longer term.

8.4 In addressing this part of IOCA, the Government will have to bear in mind the requirement of Article 6 of the European Convention on Human Rights, which guarantees the right to a fair trial. Implicit in this guarantee is the principle that there must be "equality of arms" between the prosecution and the defence in criminal proceedings. Any rule of evidence or procedure which favours one party over the other may conflict with this principle.

8.5 The question of whether section 9 of IOCA undermines the principle of "equality of arms" and introduces an unfairness into proceedings where interception played a part in the investigation was addressed by the European Commission in the case of Preston v UK[25]. The applicants claimed, amongst other things, that their trial[26] was unfair because knowledge of material gathered through interception of communications gave the prosecution an advantage in preparing their case. They also claimed that the use in evidence of data relating to communications, while interception material was excluded, amounted to an inequality of arms. The Commission did not agree, noting that section 9 prevented either party adducing evidence which could tend to suggest that interception had taken place. The Commission did not consider that the applicants had shown how access to interception material by the police had any effect on subsequent proceedings, or in what respect that material was used to the applicants' detriment in preparing the prosecution case, other than to provide the prosecuting authorities with a starting point from which to gather admissible evidence against the applicants. The Commission, by a majority, declared the application inadmissible.

[24]Cm 3420, published October 1996.

[25]Application number 24193/94 (2 July 1997).

[26]House of Lords 4 All ER 640 (1993).

8.6 In many other European states, intercept evidence is used in criminal cases and, so far as Article 6 is concerned, this practice has been approved by the European Court. See, for example, Valenzuela Contreras v Spain (30 July 1998) and Lambert v France (24 August 1998).

8.7 However, in those States interception is generally ordered by an investigating judge. The United Kingdom is in a different position, since criminal investigations are not supervised by judges but by the law enforcement agency. For that reason, the principle of equality of arms as between prosecution and defence will be particularly relevant in devising any system which allows the use of intercept material in evidence. Furthermore, any arrangements which make intercept material available to one or both parties would have to be both practical and affordable.

8.8 To date, no satisfactory arrangements have been found. Nevertheless, the Government continues to work on the question, and would welcome the views of others.

The Government welcomes suggestions for a regime which would enable intercept material to be used in evidence and to make appropriate disclosures to the defence, bearing in mind the effects upon sensitive information, resources and the efficient operation of the criminal justice system.

Chapter 9

Oversight and Redress

9.1 The need of successive governments to ensure the proper regulation of the power to intercept postal and telephone communications is made clear in the various Reports and White Papers described above. Continued public support for interception of communications can be assured only if it is clear that this intrusive means of gathering intelligence is used responsibly. For this reason Lord Diplock was appointed in 1980 in order to monitor the procedures for interception of communications on a continuing basis. In 1985 this post was placed on a statutory basis by the establishment of the Interception Commissioner by IOCA, whose duties are described in paragraph 1.8. The Government believes that the role of the Interception Commissioner is an essential one and proposes no change to this effective means of oversight.

9.2 Where a person's rights or freedoms are violated, the right to an effective remedy is established by Article 13 of the ECHR. In order to provide this means of redress, IOCA set up an independent Tribunal with full powers to investigate any case referred to it, whose duties are described in greater detail in paragraph 1.9. The Government is committed to ensuring that there will be an independent means of redress available to anyone who believes that interception has taken place unlawfully.

The Government invites comments on the oversight and redress mechanisms described above and suggestions for how their operation might be improved, bearing in mind the effects upon sensitive information and techniques.

Chapter 10

Provision of Communications Data

10.1 Because the analysis of communications data can provide much information about the way in which people live their lives, this has led to concerns that the level of intrusion into an individual's privacy may be too great and that the ability of the law enforcement, security and intelligence agencies to access this data should be regulated.

10.2 The Government believes that there is a balance to be struck between the privacy of the individual and the needs of society as a whole to be protected from crime. It is right that the police have access to communications data when necessary in order to prevent or detect crime, but only where this level of intrusion is justified, taking into account the lower level of intrusion that access to such data brings.

10.3 In recent years, advances in telecommunications have meant that the amount of data held by communications service providers has increased, making the information much more useful as an investigative tool. But so has the potential for privacy infringements. Although accessing a person's communications data is not as intrusive as interception, it clearly still represents an interference with the privacy of the individual. The Government therefore believes it is time to put in place a statutory framework for authorising access to communications data.

10.4 The Government proposes to introduce a statutorily based framework to regulate access to communications data by investigating bodies. This will lay down the purposes for which an application for access to communications data may be made, the minimum standards of information which must be included within an application and the factors which must be taken into account by the authorising official. We also propose to introduce strict statutory requirements regarding the handling, storage and retention of communications data. It is intended that these measures will be laid out in detail in the publicly available Code of Practice (see paragraph 7.16).

10.5 The proposed purposes for which data access may be authorised are:

(a) for the prevention or detection of crime;

(b) for the apprehension or prosecution of offenders;

(c) in the interests of national security;

(d) for the purpose of safeguarding the economic well-being of the United Kingdom;

(e) for the urgent prevention of injury or damage to health; and

(f) for the assessment or collection of any tax or duty or of any imposition of a similar nature.

10.6 Where a request has been properly authorised in accordance with the arrangements outlined above, the communications service provider will be required to provide the specified material within a reasonable period.

Safeguards

10.7 The disclosure of data falls within the remit of the Data Protection Act 1984 (soon to be replaced by the Data Protection Act 1998), therefore the oversight and complaints mechanisms will continue to be provided under this legislation.

The Government welcomes comments on the proposals outlined in this Chapter, particularly from Communication Service Providers and bodies which make use of communications data.

ANNEX A

QUESTIONNAIRE FOR PROVIDERS OF COMMUNICATION SERVICES

While we welcome comments on any of the Government's proposals from anyone providing communication services, it would be helpful if you could also give replies to the following questions.

1. Please describe the nature of the market you operate in and a general indication of the size and nature of your customer base.
2. Does your company fall within the scope of IOCA 1985, and if so do you compete with UK companies upon whom there is currently no intercept requirement?
3. If you are not subject to IOCA 1985, do you compete with companies who are?
4. Do you already have the capability to monitor your network where necessary for fault diagnosis or other purposes? How much additional work do you consider would be required to ensure that communications passing over your network are capable of being intercepted? What cost is involved, the nature and the scale of the cost and would it be a one-off or recurring cost?
5. Compliance costs aside, can you identify any impacts these proposals will have upon your business?
6. If you operate internationally, how do the proposed requirements compare with those placed upon you in other countries? Would it be helpful to have more consistency internationally?
7. While implementing these measures, how can the Government best support you to minimise the impact on your business?
8. Do you have any suggestions for improvements to the proposals for a framework to achieve a "reasonable intercept capability" (paras 5.3 – 5.5)?
9. What sanctions, if any, do you think would be appropriate where a CSP failed to provide a reasonable intercept capability or assistance when required by warrant? Would such sanctions assist in ensuring a level commercial playing field for comparable CSPs?
10. If you are a small – medium sized business can you comment on the ways that compliance to these proposals would be difficult or impossible?
11. Are you content for your replies to these questions to be published? YES/NO

Printed in the UK for The Stationery Office Limited on behalf of the
Controller of Her Majesty's Stationery Office
6/99 19585 J0084211 434250