Interception Code of Practice

Draft Revised Code of Practice

Interception of Communications

Code of Practice

Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000

Chapter 1
GENERAL

1.1 This code of practice relates to the powers and duties conferred or imposed under Chapter I of Part I of the Regulation of Investigatory Powers Act 2000 ("the Act"). It provides guidance on the procedures that must be followed before interception of communications can take place under those provisions. It is primarily intended for use by those public authorities listed in section 6(2) of the Act. It will also prove useful to postal and telecommunication operators and other interested bodies to acquaint themselves with the procedures to be followed by those public authorities.

1.2 The Act provides that all codes of practice relating to the Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Tribunal established under the Act, or to one of the Commissioners responsible for overseeing the powers conferred by the Act, it must be taken into account.

Chapter 2
GENERAL RULES ON INTERCEPTION WITH A WARRANT

2.1 There are a limited number of persons by whom, or on behalf of whom, applications for interception warrants may be made. These persons are:

- The Director-General of the Security Service.
- The Chief of the Secret Intelligence Service.
- The Director of GCHQ.
- The Director-General of the Serious Organised Crime Agency (SOCA handles interception on behalf of police forces in England and Wales).
- The Chief Constable of Strathclyde Police (Strathclyde Police handle interception on behalf of police forces and the SCDEA in Scotland).
- The Commissioner of the Police of the Metropolis (the Metropolitan Police Counter Terrorism Command handles some interception on behalf of Special Branches and some specialist units in England and Wales).
- The Chief Constable of the Police Service of Northern Ireland.
- The Chief Constable of any police force maintained under or by virtue of section 1 of the Police (Scotland) Act 1967.
- The Director-General of the Scottish Crime and Drug Enforcement Agency.
- The Commissioners of HM Revenue & Customs.
- The Chief of Defence Intelligence.
- A person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the United Kingdom.

Any application made on behalf of one of the above must be made by a person holding office under the Crown.

2.2 All interception warrants are issued by the Secretary of State.[1] Even where the urgency procedure is followed, the Secretary of State personally authorises the warrant, although it is signed by a senior official.

2.3 Before issuing an interception warrant, the Secretary of State must believe that what the action seeks to achieve is necessary for one of the following section 5(3) purposes:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime;
- for the purpose of safeguarding the economic well-being of the UK; and

that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

Necessity and Proportionality

[1] Interception warrants may be issued on "serious crime" grounds by Scottish Ministers, by virtue of arrangements under the Scotland Act 1998. In this Code references to the "Secretary of State" should be read as including Scottish Ministers where appropriate. The functions of the Scottish Ministers also cover renewal and cancellation arrangements.

2.4 Obtaining a warrant under the Act will only ensure that the interception authorised is a justifiable interference with an individual's rights under Article 8 of the European Convention of Human Rights (the right to privacy) if it is necessary and proportionate for the interception to take place. The Act recognises this by first requiring that the Secretary of State believes that the authorisation is necessary on one or more of the statutory grounds set out in section 5(3) of the Act. This requires him to believe that it is necessary to undertake the interception which is to be authorised for a particular purpose falling within the relevant statutory ground.

2.5 Then, if the interception is necessary, the Secretary of State must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the intrusiveness of the interference, against the need for it in operational terms. Interception of communications will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other means. Further, all interception should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Implementation of Warrants

2.6 After a warrant has been issued it will be forwarded to the person to whom it is addressed, in practice the intercepting agency which submitted the application. The Act (section 11) then permits the intercepting agency to carry out the interception, or to require the assistance of other persons in giving effect to the warrant. Warrants cannot be served on those outside the jurisdiction of the UK.

Provision of Reasonable Assistance

2.7 Any postal or telecommunications operator (referred to as communications service providers) in the United Kingdom may be required to provide assistance in giving effect to an interception. The Act places a requirement on postal and telecommunications operators to take all such steps for giving effect to the warrant as are notified to them (section 11(4) of the Act). But the steps which may be required are limited to those which it is reasonably practicable to take (section 11(5)). What is reasonably practicable should be agreed after consultation between the postal or telecommunications operator and the Government. If no agreement can be reached it will be for the Secretary of State to decide whether to press forward with civil proceedings. Criminal proceedings may also be instituted by or with the consent of the Director of Public Prosecutions.

2.8 Where the intercepting agency requires the assistance of a communications service provider in order to implement a warrant, it should provide the following to the communications service provider:

- A copy of the warrant instrument signed and dated by the Secretary of State (or in an urgent case, by a senior official);
- The relevant schedule for that service provider setting out the numbers, addresses or other factors identifying the communications to be intercepted;
- A covering document from the intercepting agency requiring the assistance of the communications service provider and specifying any other details regarding the means of interception and delivery as may be necessary. Contact details with respect to the intercepting agency will either be provided in this covering document or will be available in the handbook provided to all postal and telecommunications operators who maintain an intercept capability.

Provision of Intercept Capability

2.9 Whilst all persons who provide a postal or telecommunications service are obliged to provide assistance in giving effect to an interception, persons who provide a public postal or telecommunications service, or plan to do so, may also be required to provide a reasonable intercept capability. The obligations the Secretary of State considers reasonable to impose on such persons to ensure they have such a capability will be set out in an order made by the Secretary of State and approved by Parliament. The Secretary of State may then serve a notice upon a communications service provider setting out the steps they must take to ensure they can meet these obligations. A notice will not be served without consultation over the content of the notice between the Government and the service provider having previously taken place. When served with such a notice, a communications service provider, if he feels it unreasonable, will be able to refer that notice to the Technical Advisory Board (TAB) on the reasonableness of the technical requirements and capabilities that are being sought. Details of how to submit a notice to the TAB will be provided either before or at the time the notice is served.

2.10 Any communications service provider obliged to maintain a reasonable intercept capability will be provided with a handbook which will contain the basic information they require to respond to requests for reasonable assistance for the interception of communications.

Duration of Interception Warrants

2.11 All interception warrants are valid for an initial period of three months. Upon renewal, warrants issued on serious crime grounds are valid for a further period of three months. Warrants renewed on national security/ economic well-being grounds are valid for a further period of six months. Urgent authorisations are valid for five working days following the date of issue unless renewed by the Secretary of State.

2.12 Where modifications take place, the warrant expiry date remains unchanged. However, where the modification takes place under the urgency provisions, the modification instrument expires after five working days following the date of issue unless renewed following the routine procedure.

2.13 Where a change in circumstance prior to the set expiry date leads the intercepting agency to consider it no longer necessary or practicable for the warrant to be in force, it should be cancelled with immediate effect.

Stored Communications

2.14 Section 2(7) of the Act defines a communication in the course of its transmission as also encompassing any time when the communication is being stored on the communication system in such a way as to enable the intended recipient to have access to it. This means that a warrant can be used to obtain both communications that are in the process of transmission and those that are being stored on the transmission system.

2.15 Stored communications may also be accessed by means other than a warrant. If a communication has been stored on a communication system it may be obtained with lawful authority by means of an existing statutory power such as a production order (under the Police and Criminal Evidence Act 1984) or a search warrant.

Chapter 3
SPECIAL RULES ON INTERCEPTION WITH A WARRANT

Collateral Intrusion

3.1 Consideration should be given to any infringement of the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic, or legally privileged material may be involved, or where communications between a Member of Parliament and another person on constituency business may be involved. An application for an interception warrant should draw attention to any circumstances which give rise to an unusual degree of collateral infringement of privacy, and this will be taken into account by the Secretary of State when considering a warrant application. Should an interception operation reach the point where individuals other than the subject of the authorisation are identified as directly relevant to the operation, consideration should be given to applying for separate warrants covering those individuals.

Confidential Information

3.2 Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, communications between a Member of Parliament and another person on constituency business, confidential personal information or confidential journalistic material (see paragraphs 3.9-3.12). For example, extra consideration should be given where interception might involve communications between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

Communications Subject to Legal Privilege

3.3 Section 98 of the Police Act 1997 describes those matters that are subject to legal privilege in England and Wales. In relation to Scotland, those matters subject to legal privilege contained in section 33 of the Criminal Law (Consolidation) (Scotland) Act 1995 should be adopted. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

3.4 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the professional legal advisor is intending to hold or use the information for a criminal purpose. But privilege is not lost if a professional legal advisor is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

3.5 The Act does not provide any special protection for legally privileged communications. Nevertheless, intercepting such communications is particularly sensitive and is therefore subject to additional safeguards under this Code. The guidance set out below may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to some other material which has been sought.

3.6 In general, any application for a warrant which is likely to result in the interception of legally privileged communications should include, in addition to the reasons why it is considered necessary for the interception to take place, an assessment of how likely it is that communications which are subject to legal privilege will be intercepted. In addition, it should state whether the purpose (or one of the purposes) of the interception is to obtain privileged communications. Where the intention of the interception is not to acquire knowledge of communications subject to legal privilege, but it is likely that such knowledge will nevertheless be acquired during interception, the application should identify all steps which will be taken to mitigate the risk of acquiring it. If the risk cannot be removed entirely, the application should explain what steps will be taken to ensure that any legally privileged material obtained is not used in criminal investigations. These factors will be taken into account by the Secretary of State in deciding whether an interception is necessary under section 5(3) of the Act and whether it is proportionate. In such circumstances, the Secretary of State will be able to impose additional conditions such as regular reporting arrangements so as to be able to exercise his discretion on whether a warrant should continue to be authorised. In those cases where communications, which include legally privileged communications, have been intercepted and retained, the matter should be reported to the Interception of Communications Commissioner during his inspections and the material be made available to him if requested.

3.7 Where a lawyer is the subject of an interception, it is possible that a substantial proportion of the communications which will be intercepted will be between the lawyer and his client(s) and will be subject to legal privilege. Any case where a lawyer is the subject of an investigation should be notified to the Interception of Communications Commissioner during his inspections and any material which has been retained should be made available to him if requested.

3.8 In addition to safeguards governing the handling and retention of intercept material as provided for in section 15 of the Act, caseworkers who examine intercepted communications should be alert to any intercept material which may be subject to legal privilege. Where there is doubt as to whether the communications are subject to legal privilege, advice should be sought from a legal adviser within the intercepting agency. Similar advice should also be sought where there is doubt over whether communications are not subject to legal privilege due to the “in furtherance of a criminal purpose” exception.

Communications involving other Confidential Information

3.9 Similar consideration to that given to legally privileged communications must also be given to the interception of communications that involve confidential personal information, confidential journalistic information or communications between a Member of Parliament and another person on constituency business. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient’s medical records.

3.10 Spiritual counselling is defined as conversations between an individual and a Minister of Religion acting in his official capacity, and where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

3.11 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

3.12 References to a Member of Parliament include references to a Member of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

Chapter 4
INTERCEPTION WARRANTS (SECTION 8(l))

4.1 This section applies to the interception of communications by means of a warrant complying with section 8(l) of the Act. This type of warrant may be issued in respect of the interception of communications carried on any postal service or telecommunications system as defined in section 2(l) of the Act (including a private telecommunications system). Responsibility for the issuing of interception warrants rests with the Secretary of State

Application for a Section 8(l) Warrant

4.2 An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. This person may then serve a copy upon any person who may be able to provide assistance in giving effect to that warrant. *Prior to submission to the Secretary of State, each application shall be subject to an internal review involving scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 5(3) of the Act and whether the interception proposed is both necessary and proportionate*. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question.
- Person or premises to which the application relates (and how the person or premises feature in the operation).
- Description of the communications to be intercepted, details of the communications service provider(s) and an assessment of the feasibility of the interception operation where this is relevant.[2]
- Description of the conduct to be authorised or the conduct (including the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a) of the Act) as it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data.[3]
- An explanation of why the interception is considered to be necessary under the provisions of section 5(3).
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.
- A consideration of any unusual degree of collateral intrusion and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, or communications between a Member of Parliament and another person on constituency business, this must be specified in the application.
- Where an application is urgent, supporting justification should be provided.
- An assurance that all material intercepted will be handled in accordance with the safeguards required by section 15 of the Act.

Authorisation of a Section 8(l) Warrant

[2] This assessment is normally based upon information provided by the relevant communication service provider.
[3] Section 20 of the Act defines related communications data as being that data (within the meaning of Part I Chapter II of the Act) as is obtained by, or in connection with, the interception (under warrant); and relates to the communication to the sender or recipient, or intended recipient of the communication.

4.3 Before issuing a warrant under section 8(l), the Secretary of State must believe the warrant is necessary[4]

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of the United Kingdom.

4.4 In exercising his power to issue an interception warrant for the purpose of safeguarding the economic well-being of the United Kingdom (as provided for by section 5(3)(c) of the Act), the Secretary of State will consider whether the economic well-being of the United Kingdom which is to be safeguarded is, on the facts of each case, directly related to state security. The term "state security", which is used in Directive 97/66/EC (concerning the processing of personal data and the protection of privacy in the telecommunications sector), should be interpreted in the same way as the term "national security" which is used elsewhere in the Act and this Code. The Secretary of State will not issue a warrant on section 5(3)(c) grounds if this direct link between the economic well-being of the United Kingdom and state security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of the United Kingdom which is to be safeguarded is directly related to state security on the facts of the case.

4.5 The Secretary of State must also consider that the conduct authorised by the warrant is proportionate to what it seeks to achieve (section 5(2)(b)). In considering necessity and proportionality, the Secretary of State must take into account whether the information sought could reasonably be obtained by other means (section 5(4)).

Urgent Authorisation of a Section 8(l) Warrant

4.6 The Act makes provision (section 7(l)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to sign the warrant. In these cases the Secretary of State will still personally authorise the interception but the warrant is signed by a senior official, following discussion of the case between officials and the Secretary of State. The Act restricts issue of warrants in this way to urgent cases where the Secretary of State has himself expressly authorised the issue of the warrant (section 7(2)(a)), and requires the warrant to contain a statement to that effect (section 7(4)(a)). A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed by the Secretary of State, in which case it expires after 3 months in the case of serious crime or 6 months in the case of national security or economic well-being in the same way as other non-urgent section 8(l) warrants. An urgent case is one in which interception authorisation is required within a twenty four hour period.

Format of a Section 8(l) Warrant

4.7 Each warrant comprises two sections, a warrant instrument signed by the Secretary of State listing the subject of the interception or set of premises, a copy of which each communications service provider will receive, and a schedule or set of schedules listing the communications to be intercepted. Only the schedule relevant to the communications that can be intercepted by the specified communications service provider will be provided to that service provider.

4.8 The warrant instrument should include:

[4] A single warrant can be justified on more than one of the grounds listed.

- The name or description of the interception subject or of a set of premises in relation to which the interception is to take place.
- A warrant reference number.
- The persons who may subsequently modify the scheduled part of the warrant in an urgent case (if authorised in accordance with section 10(8) of the Act).

4.9 The scheduled part of the warrant will comprise one or more schedules. Each schedule should contain:

- The name of the communication service provider, or the other person who is to take action.
- A warrant reference number.
- A means of identifying the communications to be intercepted.[5]

Modification of Section 8(I) Warrant

4.10 Interception warrants may be modified under the provisions of section 10 of the Act. The unscheduled part of a warrant may only be modified by the Secretary of State or, in an urgent case, by a senior official with the express authorisation of the Secretary of State. In these cases, a statement of that fact must be endorsed on the modifying instrument, and the modification ceases to have effect after five working days following the day of issue unless it is renewed by the Secretary of State. The modification will then expire upon the expiry date of the warrant.

4.11 Scheduled parts of a warrant may be modified by the Secretary of State, or by a senior official[6] acting upon his behalf. A modification to the scheduled part of the warrant may include the addition of a new schedule relating to a communication service provider on whom a copy of the warrant has not been previously served. Modifications made in this way expire at the same time as the warrant expires. There also exists a duty to modify a warrant by deleting a communication identifier if it is no longer relevant. When a modification is sought to delete a number or other communication identifier, the relevant communications service provider must be advised and interception suspended before the modification instrument is signed.

4.12 In an urgent case, and where the warrant specifically authorises it, scheduled parts of a warrant may be modified by the person to whom the warrant is addressed (the person who submitted the application) or a subordinate (where the subordinate is identified in the warrant). Modifications of this kind are valid for five working days following the day of issue unless the modification instrument is endorsed by a senior official acting on behalf of the Secretary of State. Where the modification is endorsed in this way, the modification expires upon the expiry date of the warrant.

Renewal of a Section 8(I) Warrant

4.13 The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals must be made to the Secretary of State and should contain an update of the matters outlined in paragraph 4.2 above. In particular, the applicant should give an assessment of the value of interception to the operation to date and explain why he considers that interception continues to be necessary for one or more of the purposes in section 5(3).

---

[5] This may include addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying communications (section 8(2) of the Act).

[6] Neither the official, to whom the warrant is addressed, nor any of his subordinates may modify the scheduled parts of the warrant, except in an urgent case where the warrant contains an expressly authorised provision to this effect.

4.14 Where the Secretary of State is satisfied that the interception continues to meet the requirements of the Act he may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further three months. Where it is issued on national security/ economic well-being grounds, the renewed warrant is valid for six months. These dates run from the date of signature on the renewal instrument.

4.15 A copy of the warrant renewal instrument will be forwarded by the intercepting agency to all relevant communications service providers on whom a copy of the original warrant instrument and a schedule have been served, providing they are still actively assisting. A warrant renewal instrument will include the reference number of the warrant and description of the person or premises described in the warrant.

Warrant Cancellation

4.16 The Secretary of State is under a duty to cancel an interception warrant if, at any time before its expiry date, he is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of the Act. Intercepting agencies will therefore need to keep their warrants under continuous review. In practice, cancellation instruments will be signed by a senior official on his behalf.

4.17 The cancellation instrument should be addressed to the person to whom the warrant was issued (the intercepting agency) and should include the reference number of the warrant and the description of the person or premises specified in the warrant. A copy of the cancellation instrument should be sent to those communications service providers who have held a copy of the warrant instrument and accompanying schedule during the preceding twelve months.

Records

4.18 The oversight regime allows the Interception of Communications Commissioner to inspect the warrant application upon which the Secretary of State based his decision, and the applicant may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as he may require:

- all applications made for warrants complying with section 8(l) and applications made for the renewal of such warrants;
- all warrants, and renewals and copies of schedule modifications (if any);
- where any application is refused, the grounds for refusal as given by the Secretary of State;
- the dates on which interception is started and stopped.

4.19 Records shall also be kept of the arrangements by which the requirements of section 15(2) (minimisation of copying and distribution of intercepted material) and section 15(3) (destruction of intercepted material) are to be met. For further details see section on “Safeguards”.

4.20 The term “intercepted material” is used throughout to embrace copies, extracts or summaries made from the intercepted material as well as the intercept material itself.

Chapter 5
INTERCEPTION WARRANTS (section 8(4))

5.1 This section applies to the interception of external communications by means of a warrant complying with section 8(4) of the Act. External communications are defined by the Act to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transit. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. Responsibility for the issuing of such interception warrants rests with the Secretary of State.

Application for a Section 8(4) Warrant

5.2 An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. *Prior to submission, each application shall be subject to an internal review involving scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 5(3) of the Act and whether the interception proposed is both necessary and proportionate.* This person may then serve a copy upon any person who may be able to provide assistance in giving effect to that warrant. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question.
- Description of the communications to be intercepted, details of the communications service provider(s) and an assessment of the feasibility of the operation where this is relevant.[7]
- Description of the conduct to be authorised, which must be restricted to the interception of external communications, or the conduct (including the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a) of the Act) as it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data.[8]
- The certificate that will regulate examination of intercepted material.
- An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes.
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.
- A consideration of any unusual degree of collateral intrusion, and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality, legal privilege, or communications between a Member of Parliament and another person on constituency business, this must be specified in the application.
- Where an application is urgent, supporting justification should be provided.
- An assurance that intercepted material will be read, looked at or listened to only so far as it is certified, and it meets the conditions of sections 16(2)-16(6) of the Act.
- An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of the Act.

---

[7] This assessment is normally based upon information provided by the relevant communications service provider.

[8] Section 20 of the Act defines related communications data as being that data (within the meaning of Part I Chapter II of the Act) as is obtained by, or in connection with, the interception (under warrant); and relates to the communication or to the sender or recipient, or intended recipient of the communication.

Authorisation of a Section 8(4) Warrant

5.3 Before issuing a warrant under section 8(4), the Secretary of State must believe that the warrant is necessary; [9]

- in the interests of national security;
- for the purpose of preventing or detecting serious crime;
- or for the purpose of safeguarding the economic well-being of the United Kingdom.

5.4 In exercising his power to issue an interception warrant for the purpose of safeguarding the economic well-being of the United Kingdom (as provided for by section 5(3)(c) of the Act), the Secretary of State will consider whether the economic well-being of the United Kingdom which is to be safeguarded is, on the facts of each case, directly related to state security. The term "state security", which is used in Directive 97/66/EC (concerning the processing of personal data and the protection of privacy in the telecommunications sector), should be interpreted in the same way as the term "national security" which is used elsewhere in the Act and this Code. The Secretary of State will not issue a warrant on section 5(3)(c) grounds if this direct link between the economic well-being of the United Kingdom and state security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of the United Kingdom which is to be safeguarded is directly related to state security on the facts of the case.

5.5 The Secretary of State must also consider that the conduct authorised by the warrant is proportionate to what it seeks to achieve (section 5(2)(b)). In considering necessity and proportionality, the Secretary of State must take into account whether the information sought could reasonably be obtained by other means (section 5(4)).

5.6 When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate in which the Secretary of State certifies that he considers examination of the intercepted material to be necessary for one or more of the section 5(3) purposes. The Secretary of State has a duty to ensure that arrangements are in force for securing that only that material which has been certified as necessary for examination for a section 5(3) purpose, and which meets the conditions set out in section 16(2) to section 16(6) is, in fact, read, looked at or listened to. The Interception of Communications Commissioner is under a duty to review the adequacy of those arrangements.

Urgent Authorisation of a Section 8(4) Warrant

5.7 The Act makes provision (section 7(l)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to sign the warrant. In these cases the Secretary of State will still personally authorise the interception but the warrant is signed by a senior official, following discussion of the case between officials and the Secretary of State. The Act restricts issue of warrants in this way to urgent cases where the Secretary of State has himself expressly authorised the issue of the warrant (section 7(2)(a)), and requires the warrant to contain a statement to that effect (section 7(4)(a)).

5.8 A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed by the Secretary of State, in which case it expires after 3 months in the case

[9] A single warrant can be justified on more than one of the grounds listed.

of serious crime or 6 months in the case of national security or economic well-being in the same way as other section 8(4) warrants.

Format of a Section 8(4) Warrant

5.9 Each warrant is addressed to the person who submitted the application. This person may then serve a copy upon such providers of communications services as he believes will be able to assist in implementing the interception. Communications service providers will not receive a copy of the certificate. The warrant should include the following:

- A description of the communications to be intercepted.
- The warrant reference number.
- The persons who may subsequently modify the certificate applicable to the warrant in an urgent case (if authorised in accordance with section 10(7) of the Act).

Modification of a section 8(4) Warrant and/or certificate

5.10 Interception warrants may be modified under the provisions of section 10 of the Act. The warrant may only be modified by the Secretary of State or, in an urgent case, by a senior official with the express authorisation of the Secretary of State. In these cases a statement of that fact must be endorsed on the modifying instrument, and the modification ceases to have effect after five working days following the day of issue unless it is endorsed by the Secretary of State.

5.11 The certificate must be modified by the Secretary of State, save in an urgent case where a certificate may be modified under the hand of a senior official provided that the official holds a position in respect of which he is expressly authorised by provisions contained in the certificate to modify the certificate on the Secretary of State's behalf, or the Secretary of State has himself expressly authorised the modification and a statement of that fact is endorsed on the modifying instrument. In the latter case the modification shall cease to have effect after five working days following the day of issue unless it is endorsed by the Secretary of State.

5.12 Where the requirements of section 16(3) of the Act are met, the certificate may be modified to authorise the selection of communications sent or received outside the British Islands according to a factor which is referable to an individual who is known for the time being to be in the British Islands and which has as its purpose, or one of its purposes, the identification of material contained in communications sent by him or intended for him.

Renewal of a Section 8(4) Warrant

5.13 The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 5.2 above. In particular, the applicant must give an assessment of the value of interception to date and explain why it is considered that interception continues to be necessary for one or more of the purposes in section 5(3).

5.14 Where the Secretary of State is satisfied that the interception continues to meet the requirements of the Act he may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further three months. Where it is issued on national security/ economic well-being grounds the renewed warrant is valid for six months. These dates run from the date of signature on the renewal instrument.

5.15 In those circumstances where the assistance of communications service providers has been sought, a copy of the warrant renewal instrument will be forwarded by the intercepting agency to

all those on whom a copy of the original warrant instrument has been served, providing they are still actively assisting. A warrant renewal instrument will include the reference number of the warrant and a description of the communications to be intercepted.

Warrant Cancellation

5.16 The Secretary of State shall cancel an interception warrant if, at any time before its expiry date, he is satisfied that the warrant is no longer necessary on grounds falling within Section 5(3) of the Act. In practice, cancellation instruments will be signed by a senior official on his behalf

5.17 The cancellation instrument will be addressed to the person to whom the warrant was issued (the intercepting agency). A copy of the cancellation instrument should be sent to those communications service providers, if any, who have given effect to the warrant during the preceding twelve months.

Records

5.18 The oversight regime allows the Interception of Communications Commissioner to inspect the warrant application upon which the Secretary of State based his decision, and the applicant may be required to justify the content. Each intercepting agency should keep, so to be made available for scrutiny by the Interception of Communications Commissioner, the following:

- all applications made for warrants complying with section 8(4), and applications made for the renewal of such warrants;
- all warrants and certificates, and copies of renewal and modification instruments (if any);
- where any application is refused, the grounds for refusal as given by the Secretary of State;
- the dates on which interception is started and stopped.

Records shall also be kept of the arrangements in force for securing that only material which has been certified for examination for a purpose under section 5(3) and which meets the conditions set out in section 16(2) – 16(6) of the Act in accordance with section 15 of the Act. Records shall be kept of the arrangements by which the requirements of section 15(2) (minimisation of copying and distribution of intercepted material) and section 15(3) (destruction of intercepted material) are to be met. For further details see section on “Safeguards”.

Chapter 6
SAFEGUARDS

6.1 All material intercepted under the authority of a warrant complying with section 8(l) or section 8(4) of the Act and any related communications data[10] must be handled in accordance with safeguards which the Secretary of State has approved in conformity with the duty imposed upon him by the Act. These safeguards are made available to the Interception of Communications Commissioner, and they must meet the requirements of section 15 of the Act which are set out below. In addition, the safeguards in section 16 of the Act apply to warrants complying with section 8(4). Any breach of these safeguards must be reported to the Interception of Communications Commissioner.

6.2 Section 15 of the Act requires that disclosure, copying and retention of intercept material be limited to the minimum necessary for the authorised purposes. The authorised purposes defined in section 15(4) of the Act include:

- if the material continues to be, or is likely to become, necessary for any of the purposes set out in section 5(3) – namely, in the interests of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic wellbeing of the United Kingdom;
- if the material is necessary for facilitating the carrying out of the functions of the Secretary of State under Chapter I of Part I of the Act;
- if the material is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or the Tribunal;
- if the material is necessary to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution;
- if the material is necessary for the performance of any duty imposed by the Public Record Acts.

6.3 Section 16 provides for additional safeguards in relation to material gathered under section 8(4) warrants, requiring that the safeguards:

- ensure that intercepted material is read, looked at or listened to by any person only to the extent that the material is certified;
- regulate the use of selection factors that refer to individuals known to be for the time being in the British Islands.

6.4 Material gathered under a section 8(4) warrant should be read, looked at or listened to only by authorised persons who receive regular mandatory training regarding the provisions of the Act and specifically the operation of section 16 and the requirements of necessity and proportionality.

6.5 In general, automated systems must where technically possible be used to process and filter the volumes of material that are gathered under section 8(4) warrants so as to select the material

[10] Under section 20 of the Act related communications data means so much of any communications data (within the meaning of Chapter II of Part I of the Act) as is obtained by, or in connection with, the interception (under warrant); and relates to the communication or to the sender or recipient, or intended recipient, of the communication.

that is accessed by persons (in the sense of being read, looked at or listened to) in accordance with section 16(1) of the Act. As an exception to this, intercepted material may be accessed by a limited number of specifically authorised staff without first having been processed or filtered by automated systems when this is necessary to determine whether the material so checked is capable of falling within the main categories to be selected under the certificate in question or to ensure the continued efficacy of the systems used. Further, material may only be accessed in this way when such access is expressly provided for by the certificate in question.

6.6 Prior to an authorised person being able to read, look at or listen to material, a record[11] should be created setting out why access to the material is necessary and proportionate and required for a specific purpose falling within section 5(3) of the Act. Save where the automated systems are being checked as described in the previous paragraph, the record must indicate by reference to specific factors the material to which access is being sought and systems should, to the extent possible, prevent access to the material unless such a record has been created. Access to the material must be limited to a defined period of time, although access may be renewed. If access is renewed, the record must be updated with the reason for renewal. Systems must be in place to ensure that if a request for renewal is not made within that period then no further access will be granted. When access to the material is no longer sought, the reason for this must also be explained in the record.

6.7 Periodic audits should be carried out by authorised persons to ensure that the requirements set out in section 16 of the Act are being met. This audit must include checks to ensure that the records requesting access to material to be read, looked at, or listened to have been correctly compiled and specifically that the material requested falls within matters certified by the Secretary of State. Any errors or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious breaches should also be brought to the attention of senior management and any breaches of the Act reported to the Interception of Communications Commissioner.

6.8 In order to meet the requirements of the Act as described in paragraph 5.11 above, where a selection factor refers to an individual known to be for the time being in the British Islands and has as its purpose, or one of its purposes, the identification of material contained in communications sent by him or intended for him, a submission shall be made giving an explanation why an amendment to the section 8(4) certificate in relation to such an individual is necessary for a purpose falling within section 5(3) of the Act and is proportionate in relation to any conduct authorised under section 8(4) of the Act.

6.9 The Secretary of State must ensure that the safeguards are in force before any interception under section 8(4) warrants can begin. The Interception of Communications Commissioner is under a duty to review the adequacy of the safeguards.

Dissemination of Intercepted Material

6.10 The number of persons to whom any of the material is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of the Act. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he needs to know about the material to

[11] Which can be made available on request to the Commissioner for purposes of oversight.

carry out those duties. In the same way only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

6.11 The obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

Copying

6.12 Intercepted material may only be copied to the extent necessary for the authorised purposes set out in section 15(4) of the Act. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.

Storage

6.13 Intercepted material, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store intercept product securely applies to all those who are responsible for the handling of this material, including communications service providers. The details of what such a requirement will mean in practice for communications service providers will be set out in the discussions they will be having with the Government before a Section 12 Notice is served (see paragraph 2.9).

Destruction

6.14 Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorised purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 15(3) of the Act.

Personnel security

6.15 Each intercepting agency maintains a distribution list of persons who may have access to intercepted material or need to see any reporting in relation to it. All such persons must be appropriately vetted. Any person no longer needing access to perform his duties should be removed from any such list. Where it is necessary for an officer of one agency to disclose material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

Chapter 7
DISCLOSURE TO ENSURE FAIRNESS IN CRIMINAL PROCEEDINGS

7.1 Section 15(3) of the Act states the general rule that intercepted material must be destroyed as soon as its retention is no longer necessary for a purpose authorised under the Act. Section 15(4) specifies the authorised purposes for which retention is necessary.

7.2 This part of the Code applies to the handling of intercepted material in the context of criminal proceedings where the material has been retained for one of the purposes authorised in section 15(4) of the Act. For those who would ordinarily have had responsibility under the Criminal Procedure and Investigations Act 1996 to provide disclosure in criminal proceedings, this includes those rare situations where destruction of intercepted material has not taken place in accordance with section 15(3) and where that material is still in existence after the commencement of a criminal prosecution, retention having been considered necessary to ensure that a person conducting a criminal prosecution has the information he needs to discharge his duty of ensuring its fairness (section 15(4)(d)).

Exclusion of Matters from Legal Proceedings

7.3 The general rule is that neither the possibility of interception nor intercepted material itself plays any part in legal proceedings. This rule is set out in section 17 of the Act, which excludes evidence, questioning, assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under this Act (or the Interception of Communications Act 1985). This rule means that the intercepted material cannot be used either by the prosecution or the defence. This preserves “equality of arms” which is a requirement under Article 6 of the European Convention on Human Rights.

7.4 Section 18 contains a number of tightly-drawn exceptions to this rule. This part of the Code deals only with the exception in subsections (7) to (11).

Disclosure to a Prosecutor

7.5 Section 18(7)(a) provides that intercepted material obtained by means of a warrant and which continues to be available, may, for a strictly limited purpose, be disclosed to a person conducting a criminal prosecution.

7.6 This may only be done for the purpose of enabling the prosecutor to determine what is required of him by his duty to secure the fairness of the prosecution. The prosecutor may not use intercepted material to which he is given access under section 18(7)(a) to mount a cross-examination, or to do anything other than ensure the fairness of the proceedings.

7.7 The exception does not mean that intercepted material should be retained against a remote possibility that it might be relevant to future proceedings. The normal expectation is, still, for the intercepted material to be destroyed in accordance with the general safeguards provided by

section 15. The exceptions only come into play if such material has, in fact, been retained for an authorised purpose. Because the authorised purpose given in section 5(3)(b) ("*for the purpose of preventing or detecting serious crime*") does not extend to gathering evidence for the purpose of a prosecution, material intercepted for this purpose may not have survived to the prosecution stage, as it will have been destroyed in accordance with the section 15(3) safeguards. There is, in these circumstances, no need to consider disclosure to a prosecutor if, in fact, no intercepted material remains in existence.

7.8 Be that as it may, section 18(7)(a) recognises the duty on prosecutors, acknowledged by common law, to review all available material to make sure that the prosecution is not proceeding unfairly.'Available material' will only ever include intercepted material at this stage if the conscious decision has been made to retain it for an authorised purpose.

7.9 If intercepted material does continue to be available at the prosecution stage, once this information has come to the attention of the holder of this material the prosecutor should be informed that a warrant has been issued under section 5 and that material of possible relevance to the case has been intercepted.

7.10 Having had access to the material, the prosecutor may conclude that the material affects the fairness of the proceedings. In these circumstances, he will decide how the prosecution, if it proceeds, should be presented.

Disclosure to a Judge

7.11 Section 18(7)(b) recognises that there may be cases where the prosecutor, having seen intercepted material under subsection (7)(a), will need to consult the trial Judge. Accordingly, it provides for the Judge to be given access to intercepted material, where there are exceptional circumstances making that disclosure essential in the interests of justice.

7.12 This access will be achieved by the prosecutor inviting the judge to make an order for disclosure to him alone, under this subsection. This is an exceptional procedure; normally, the prosecutor's functions under subsection (7)(a) will not fall to be reviewed by the judge. To comply with section 17(l), any consideration given to, or exercise of, this power must be carried out without notice to the defence. The purpose of this power is to ensure that the trial is conducted fairly.

7.13 The judge may, having considered the intercepted material disclosed to him, direct the prosecution to make an admission of fact. The admission will be abstracted from the interception; but, in accordance with the requirements of section 17(l), it must not reveal the fact of interception. This is likely to be a very unusual step. The Act only allows it where the judge considers it essential in the interests of justice.

7.14 Nothing in these provisions allows intercepted material, or the fact of interception, to be disclosed to the defence.

Chapter 8
OVERSIGHT

8.1 The Act provides for an Interception of Communications Commissioner whose remit is to provide independent oversight of the use of the powers contained within the warranted interception regime under Chapter I of Part I of the Act.

8.2 This Code does not cover the exercise of the Commissioner's functions. However, any person who exercises the above powers must report any action that is believed to be contrary to the provisions of the Act to the Commissioner and comply with any request made, by the Commissioner to provide such any information as the Commissioner requires for the purpose of enabling him to discharge his functions.

Chapter 9
COMPLAINTS

9.1 The Act establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

9.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:
The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ
☎ 0207 035 3711

Chapter 10
INTERCEPTION WITHOUT A WARRANT

10.1 Section 1(5) of the Act permits interception without a warrant in the following circumstances:

- where it is authorised by or under sections 3 or 4 of the Act (see below);
- where it is in exercise, in relation to any stored communication, of some other statutory power exercised for the purpose of obtaining information or of taking possession of any document or other property, for example, the obtaining of a production order under Schedule 1 to the Police and Criminal Evidence Act 1984 for stored data to be produced.

Interception in accordance with a warrant under section 5 of the Act is dealt with under parts 2, 3, 4 and 5 of this Code.

10.2 For lawful interception which takes place without a warrant, pursuant to sections 3 or 4 of the Act or pursuant to some other statutory power, there is no prohibition in the Act on the evidential use of any material that is obtained as a result. The matter may still, however, be regulated by the exclusionary rules of evidence to be found in the common law, section 78 of the Police and Criminal Evidence Act 1984, and/or pursuant to the Human Rights Act 1998.

Interception with the Consent of both Parties

10.3 Section 3(l) of the Act authorises the interception of a communication if both the person sending the communication and the intended recipient(s) have consented to its interception.

Interception with the Consent of one Party

10.4 Section 3(2) of the Act authorises the interception of a communication if either the sender or intended recipient of the communication has consented to its interception, and directed surveillance by means of that interception has been authorised under Part II of the Act or authorised under The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA). Further details can be found in chapter 2 of the Covert Surveillance Code of Practice and in chapter 3 of the Covert Human Intelligence Sources Code of Practice, or their RIPSA equivalents**.**

Interception for the Purposes of a Communication Service Provider

10.5 Section 3(3) of the Act permits a communication service provider or a person acting upon their behalf to carry out interception for purposes connected with the operation of that service or for purposes connected with the enforcement of any enactment relating to the use of the communication service.

Lawful Business Practice

10.6 Section 4(2) of the Act enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept communications for the purpose of carrying on a business. These regulations apply equally to public authorities. These Lawful Business Practice

Regulations can be found on the following Department for Business, Innovation and Skills website:
http://www.opsi.gov.uk/si/si2000/uksi_20002699_en.pdf

Alternative Formats

If you require a copy of this consultation paper in any other format, e.g. Braille, Large Font, or Audio', please contact us in writing at the following address;

Anjna Parmar/ J Krishnan
Home Office
5th Floor Peel Building
2 Marsham Street
London SW1P 4DF

Or by email at InterceptionCode@homeoffice.gsi.gov.uk

The Department is obliged to both offer, and provide on request, these formats under the Disability Act so you will need to prepare for this situation.

ANNEX A

Responses: Confidentiality & Disclaimer

The information you send us may be passed to colleagues within the Home Office, the Government or related agencies.

Information provided in response to this consultation, including personal information, may be subject to publication or disclosure in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 [FOIA], the Data Protection Act 1998 [DPA] and the Environmental Information Regulations 2004).

If you want other information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence.

In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

The Department will process your personal data in accordance with the DPA and in the majority of circumstances this will mean that your personal data will not be disclosed to third parties.'

Consultation Criteria

The Consultation follows the Government's Code of Practice on Consultation – the criteria for which are set out below:

Criterion 1 – When to consult – Formal consultation should take place at a stage when there is scope to influence the policy outcome.

Criterion 2 – Duration of consultation exercises – Consultations should normally last for at least 12 weeks with consideration given to longer timescales where feasible and sensible.

Criterion 3 – Clarity of scope and impact – Consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals.

Criterion 4 – Accessibility of consultation exercises – Consultation exercises should be designed to be accessible to, and clearly targeted at, those people the exercise is intended to reach.

Criterion 5 – The burden of consultation – Keeping the burden of consultation to a minimum is essential if consultations are to be effective and if consultees' buy-in to the process is to be obtained.

Criterion 6 – Responsiveness of consultation exercises – Consultation responses should be analysed carefully and clear feedback should be provided to participants following the consultation.

Criterion 7 – Capacity to consult – Officials running consultations should seek guidance in how to run an effective consultation exercise and share what they have learned from the experience.

The full Code of Practice on Consultation is available at:
http://www.berr.gov.uk/whatwedo/bre/consultation-guidance/page44420.html

Consultation Co-ordinator

If you have a complaint or comment about the Home Office's approach to consultation, you should contact the Home Office Consultation Co-ordinator, Nigel Lawrence. Please DO NOT send your response to this consultation to Nigel Lawrence. The Co-ordinator works to promote best practice standards set by the Government's Code of Practice, advises policy teams on how to conduct consultations and investigates complaints made against the Home Office. He does not process your response to this consultation.

The Co-ordinator can be emailed at: Nigel.Lawrence@homeoffice.gsi.gov.uk or alternatively write to him at:

Nigel Lawrence, Consultation Co-ordinator

Home Office
Performance and Delivery Unit
Better Regulation Team
3rd Floor Seacole
2 Marsham Street
London
SW1P 4DF