DRAFT

INTERCEPTION OF COMMUNICATIONS AND ACCESSING COMMUNICATIONS DATA

DRAFT CODE OF PRACTICE

Preliminary draft code: This document is circulated by the Home Office in advance of enactment of the RIP Bill as an indication of current thinking. It will be subject to changes and additions. This circulation is not the publication referred to in clause 69(3) of the Bill, which can only take place after enactment. This is a preliminary draft on which comments are welcomed. Further, informal consultation will be required before the formal consultation process begins under clause 69(3) of the Bill.

DRAFT

CONTENTS

1 GENERAL

1.1 This code of practice provides guidance on the use of interception of communications and accessing communications data authorised under Part I of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"). It covers operations conducted by all the public authorities listed in these parts of the 2000 Act.

1.2 A copy of the Code should be readily available, for reference purposes, at public offices of public authorities designated to carry out interception or accessing communications data, and where people are detained in custody. It should also be readily available to any members of an agency or department who are actively involved in interception operations or accessing communications data.

1.3 The 2000 Act provides that the Code is admissible as evidence in criminal and civil proceedings. If any provision of the Code appears relevant to any court or tribunal considering any such proceedings, it must be taken into account.

2 AUTHORISATIONS

2.1 Any person giving an authorisation should first satisfy himself that what the action seeks to achieve is necessary and that the degree of infringement of the privacy of those affected by interception is proportionate. The fullest consideration should be given in cases where the subject of the interception might reasonably assume a high degree of privacy or where there are special sensitivities, such as where interception might involve communications between a minister of any religion or faith and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal professional privilege may be involved. [further guidelines are being drafted and will be incorporated in final version]

2.2 Particular consideration should be given to any infringement of the privacy of individuals other than the object of interception, especially where communications concerning any form of medical or professional counselling or therapy may be involved. An application for interception should include an assessment of the risk of any collateral infringement of privacy and this should be taken into account by the person giving the authorisation when considering the proportionality of the action. 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 must be given to applying for separate authorisations to cover those individuals.

CHAPTER I - INTERCEPTION OF COMMUNICATIONS

3. EXCEPTIONS TO THE WARRANTRY REGIME

3.1 Section 1(5) of the Act permits interception in the following circumstances:

- where it is authorised by or under section 3 or 4;
- where it takes place in accordance with a warrant under section 5; or
- 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.

Interception in accordance with a warrant under section 5 is dealt with under Part Four of this Code.

Because interception which takes place under the exceptions to the warrantry regime is not warranted by the Secretary of State there is no prohibition on the evidential use of material gathered in accordance with the provisions described in this part of this Code.

Interception with the consent of both parties

3.2 Section 3(1) 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, or where the person conducting the interception has reasonable grounds for believing that both parties have consented to the interception.

Interception with the consent of one party

3.3 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 surveillance by means of that interception has been authorised under Part II of the Act.

3.4 This surveillance is therefore regulated by Part II of the Act, and not by Part I. It is dealt with in the Covert Surveillance Code of Practice at paragraph 3.17 and the Covert Human Intelligence Sources Code of Practice at paragraph 2.28.

Lawful business practice

3.5 Section 4(2) of the Act authorises conduct, in connection with the carrying on of any business, of monitoring or keeping a record of communications by means of which transactions are entered into in the course of

that business, or other communications relating to that business or taking place in the course of its being carried on.

[The remainder of this section is subject to the public consultation exercise which is to be undertaken on the scope and content of regulations to be made under section 4(2)]

Interception for the purposes of a communication service provider

3.6 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.

This provision does not allow the police or other law enforcement bodies to carry out interception.

4. INTERCEPTION WITH A WARRANT

4.1 There are two types of interception warrants which may be authorised under the 2000 Act, both of which must be personally authorised by the Secretary of State[1]. There are a small number of persons by whom, or on behalf of whom[2], applications for interception warrants may be submitted. The 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 National Criminal Intelligence Service (NCIS handle interception on behalf of police forces in England and Wales).
- The Commissioner of the Police of the Metropolis (the Metropolitan Police handle interception on behalf of Special Branches).
- The Chief Constable of the Royal Ulster Constabulary.
- The Chief Constable of any police force maintained under or by virtue of section 1 of the Police (Scotland) Act 1967 (the Scottish Recording Centre is maintained by the Scottish Executive and each Chief Constable makes applications direct to the Executive where "prevention or detection of serious crime" warrants are sought); footnote saying that this will be achieved by an Order in Council under section 63 of the Scotland Act.
- The Commissioners of Customs and Excise.
- The Chief of Defence Intelligence.
- A person who, for the purposes of any international mutual assistance agreements, is the competent authority of a country or territory outside the United Kingdom.

4.2 All interception warrants are authorised personally by the Secretary of State[3]. The vast majority of these are section 8(1) warrants, in order to intercept the communications of a person or premises located within the British Islands.

4.3 The remaining warrants, again personally authorised by the Secretary of State, are warrants authorised under section 8(4) in order to intercept external communications, which 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.

[1] **Guidance note:** Interception warrants issued on "serious crime" grounds are authorised by the First Minister in Scotland.

[2] **Guidance note:** The list of persons is set out in section 6(2) of the Act: it is a further requirement that all such applications be made by a person holding office under the Crown.

[3] **Guidance note:** Even where the urgency procedure is followed, the Secretary of State personally authorises the warrant, although it is signed by a Senior Civil Servant. See para 5.4.

Implementation of warrants

4.4 After a warrant has been authorised it is served upon the person to whom it is addressed, in practice the intercepting agency which submitted the application. The Act then allows the intercepting agency to carry out the interception themselves, or to require the assistance of other persons in giving effect to the warrant (section 11(1)).

Provision of reasonable assistance

4.5 Any provider of a communication service in the United Kingdom may be required to provide assistance in effecting an interception on their communication system. The Act places a requirement to take all such steps for giving effect to the warrant as are notified to them (section 11(4)). But the steps which may be required of a communication service provider are limited to those which it is reasonably practical (section 11(5)).

4.6 Where the intercepting agency requires the assistance of a communication service provider in order to implement a warrant, they will provide the following to the communication service provider:

- A copy of the relevant portions of the warrant (see paragraph 5.5)
- Notification of the steps which the intercepting agency is requiring them to undertake.

Provision of intercept capability

4.7 The persons who may be required to provide an intercept capability are persons providing a public postal or telecommunications service (communication service providers), or who plan to do so. These persons may have a notice served upon them by the Secretary of State under section 12(2) of the Act, which must fall within the scope of any order made in Parliament by the Secretary of State, setting out in more general terms the requirements for providing assistance with interception warrants. No communication service provider is required to provide an intercept capability unless they have been served with a notice under section 12(2).

4.8 Individual notices served on particular communication service providers under this order may specify:

- what practical capability for providing assistance with interception warrants is required.
- what arrangements should be in place with regard to the disclosure of intercepted material.
- how security and confidentiality are to be maintained.
- what measures should be in place to facilitate the carrying out of the functions of the Interception of Communications Commissioner.

Duration of interception warrants

4.9 All interception warrants on serious crime grounds are valid for an initial period of three months. Upon renewal, warrants authorised on serious crime grounds are valid for a further period of three months. Warrants authorised on national security or economic well-being grounds are valid for six months. Urgent authorisations are valid for five working days unless endorsed by the Secretary of State.

4.10 Where modifications take place, the warrant expiry date remains unchanged. However, where the modification took place following the urgency provisions, the modification instrument expires after five working days unless endorsed following the routine procedure. These matters are expanded upon in the sections dealing with interception warrants below.

5. SECTION 8(1) WARRANTS

5.1 This section applies to interception of communications by means of a warrant complying with section 8(1) of the 2000 Act. Such a warrant may be issued in respect of the interception of communications carried on public or private telecommunications systems (as defined in section 2(1) of the Act). Responsibility for the authorisation of all such interception rests with the Secretary of State.

Application for 8(1) warrant

5.2 The Secretary of State will make a decision whether to grant a warrant based upon the application which is made. The application is not served upon communication service providers; the warrant which they receive contains only enough information to allow them to fulfil their duties under the Act (see). But in his oversight of the Secretary of State's use of his powers granted under the Act, the Commissioner may inspect the application upon which the Secretary of State based his decisions, and the applicant may be required to justify the content. Applications for warrants, a copy of which must be retained by applicant, must contain the following minimum information:

- Background to the operation.
- Person or premises to which the application relates and how the person or premises features in the operation.
- Description of the communications to be intercepted, details of the communication service provider(s) and an assessment of the feasibility of this particular interception operation[4].
- An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes.
- A consideration of the proportionality implications and a justification of why interception of communications constitutes a proportionate response to the threat posed.
- A consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified. In particular where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.
- A consideration of why the material sought through interception could not be achieved by other less intrusive means.
- An indication of the urgency of the application with supporting justification.
- An assurance that all material intercepted will be handled in accordance with the safeguards required by section 14 of the Act.

Authorisation of 8(1) warrant

[4] **Guidance note:** this assessment is normally based upon information provided by the relevant communication service provider.

5.3 Before granting a warrant under section 8(1), the Secretary of State must be satisfied that the criteria demanded by the Act are fulfilled, namely the warrant is necessary[5]

- in the interests of national security;
- for the purpose of preventing and detecting serious crime; or
- for the purpose of safeguarding the economic well-being of the United Kingdom[6].

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)).
- whether the information sought could reasonably be obtained by other means. (section 5(4)).

Urgent authorisation of 8(1) warrants

5.4 The Act makes provision (section 7(1)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to personally sign the warrant. In these cases the Secretary of State still personally authorises the interception but the warrant is issued 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 unless endorsed by the Secretary of State, in which case it expires after 3 months in the same way as other 8(1) warrants, unless renewed.

Format of 8(1) warrant

5.5 Interception warrants are addressed to the person who submitted the application who may then serve a copy upon such providers of communication services as he believes will be able to assist in implementing the interception. Each warrant comprises two sections, an unscheduled part, a copy of which each communication service provider will receive, and a scheduled part, only the relevant part of which each communication service provider will receive.

5.6 The unscheduled part will include the following elements:

- The name of the person to be intercepted, or a description of the premises
- The warrant reference number
- The persons who may subsequently modify the scheduled part of the warrant (if applicable)
- Contact details so that the veracity of the warrant may be checked

[5] **Guidance note:** A single warrant can be justified on more than one of the grounds listed.
[6] **Guidance note:** The information sought must relate to the acts or intentions of persons outside the British Islands (section 5(2)(a)).

5.7 The scheduled part of the warrant, which will be one or more schedules, will contain:

- The name of the communication service provider
- The warrant reference number
- A means of identifying the communications to be intercepted[7]

5.8 Interception warrants may be modified under the provisions of section 10. The unscheduled parts of warrants 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 unless it is endorsed by the Secretary of State's personal signature. Otherwise the modification expires upon the expiry date of the warrant.

5.9 Scheduled parts of an 8(1) interception warrant may be modified by the Secretary of State, or by a senior official[8] acting upon his behalf. Modifications made in this way expire at the same time as the warrant expires.

5.10 In an urgent case, scheduled parts of a warrant may be modified by the person to whom the warrant is addressed or a subordinate (where the subordinate is identified in the warrant). Modifications of this kind last for five working days unless the modification instrument is endorsed by the Secretary of State or by a senior official acting on his behalf. Where the modification is endorsed in this way, the modification expires upon the expiry date of the warrant.

Renewal of 8(1) warrants

5.11 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 the operation to date and explain why he considers that interception continues to be necessary for the section 5(3) purposes.

5.12 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 was issued on serious crime grounds, the renewed warrant is valid for a further three months, where it was issued on national security or economic well-being grounds the renewed warrant is valid for six months.

[7] **Guidance note:** This may include addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying communications (section 8(2)).

[8] **Guidance note:** The senior official who may modify the unscheduled part of the warrant may not be the person to whom the warrant is addressed, nor any of their subordinates (s10(6)).

Records

5.13 A record, which shall be available for scrutiny by the Interception Commissioner, should be retained of:

- all applications made for warrants complying with section 8(1), for the renewal of such warrants, or for the modification of warrants, including the matters listed in paragraph 5.2.
- the signed originals of all warrants, and 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.

8(1) warrants under mutual legal assistance agreements

5.14 The Act makes provision for two sets of circumstances in which interception assistance may be given in support of a mutual legal assistance agreement, where the agreement has been designated by the Secretary of State in an order under section 1(4)(c) of the Act. The first is where the person under investigation is in the United Kingdom and the competent authorities of another country believe it is necessary to intercept that person's communications. The second situation is where the person being investigated is not in the United Kingdom but the competent authorities of another country nevertheless require the assistance of a communication service provider in the UK in order to intercept their communications. Both of these situations require an 8(1) warrant to be issued before interception could take place, and the paragraphs below explain the levels of authority required.

5.15 Where the person under investigation is in the UK, the country requesting assistance must apply to the Secretary of State in much the same way as any other application under section 8(1), following the procedure described in paragraph 5.2. The Secretary of State may not issue a warrant for the purposes of a mutual assistance agreement unless the circumstances are equivalent to those in which he would issue a warrant for the prevention or detection of serious crime (section 5(3)(d).

5.16 Where the person under investigation is on the territory of the requesting country and only requires the technical assistance of a communication service provider in the UK in order to effect the interception, a senior official may issue an interception warrant under section 7(2)(b). Where a warrant is authorised in this way, it must contain the statement required by section 7(4)(b) explaining the provisions under which it has been issued.

6. SECTION 8(4) (EXTERNAL) WARRANTS

6.1 This section applies to the interception of external communications by means of a warrant complying with section 8(4) of the Regulation of Investigatory Powers Act 2000. 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.

6.2 Such a warrant may be issued in respect of the interception of communications carried on public or private telecommunications systems (as defined in section 2(1) of the Act). Responsibility for the authorisation of all such interception rests with the Secretary of State.

Application for 8(4) warrants

6.3 The Secretary of State will make a decision whether to grant a warrant based upon the application which is made. The application is not served upon communication service providers, the warrant which they receive contains only enough information to allow them to fulfil their duties under the Act (see 5.5 above). But in his oversight of the Secretary of State's use of his powers granted under the Act, the Commissioner may inspect the application upon which the Secretary of State based his decisions, and the applicant may be required to justify the content. Applications for warrants, a copy of which must be retained by the applicant, must contain the following minimum information:

- Background to the operation.
- Description of the communications to be intercepted, details of the communication service provider(s) and an assessment of the feasibility of this particular interception operation[9].
- Description of the conduct to be authorised, which must be restricted to the interception of external communications, or to conduct necessary[10] in order to intercept those external communications.
- A copy of 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 the proportionality implications and a justification of why interception of communications constitutes a proportionate response to the threat posed.
- A consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified. In particular where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.
- A consideration of why the material sought through interception could not be achieved by other less intrusive means.
- An indication of the urgency of the application with supporting justification;

[9] **Guidance note:** This assessment is normally based upon information provided by the relevant communication service provider.

[10] **Guidance note:** This conduct may include the interception of other communications (section 5(6)(a)).

- An assurance that intercepted material will only be read, looked at or listened to only so far as it is certified, and it meets the conditions of sections 15(2)-15(6) of the Act.
- An assurance that all material intercepted will be handled in accordance with the safeguards required by section 14 of the Act.

Authorisation of 8(4) warrants

6.4 Before granting a warrant under section 8(4), the Secretary of State must be satisfied that the criteria demanded by the Act are fulfilled, namely the warrant is necessary[11]

- in the interests of national security;
- for the purpose of preventing and detecting serious crime; or
- for the purpose of safeguarding the economic well-being of the United Kingdom[12];

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)).
- whether the information sought could reasonably be obtained by other means. (section 5(4)).

6.5 When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate by which the Secretary of State certifies that he considers examination of intercepted material necessary for one or more of the purposes listed in paragraph 6.4. The Secretary of State has a duty to ensure that there are arrangements in force for securing that only that material which has been certified as necessary for examination for a national security etc purpose is, in fact, read, looked at or listened to. The Interception Commissioner is under a duty to review the adequacy of those arrangements (see paragraph 10.1 below)[13].

Urgent authorisation of 8(4) warrants

6.6 The Act makes provision (section 7(1)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to personally sign the warrant. In these cases the Secretary of State still personally authorises the interception but the warrant is issued 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)).

[11] **Guidance note:** A single warrant can be justified on more than one of the grounds listed.
[12] **Guidance note:** The information sought must relate to the acts or intentions of persons outside the British Islands (section 5(2)(a)).
[13] **Guidance note:** These arrangements are called safeguards in the Act and in this Code.

6.7 A warrant issued under the urgency procedure lasts for five working days unless endorsed by the Secretary of State, in which case it expires after 3 months in the same way as other 8(4) warrants, unless renewed.

Format of 8(4) warrant

6.8 Interception warrants are addressed to the person who submitted the application who may then serve a copy upon such providers of communication services as he believes will be able to assist in implementing the interception. Communication service providers will not receive a copy of the certificate.

The warrant should include the following elements:

- A description of the communications to be intercepted.
- The warrant reference number
- The name of the communication service provider(s)
- Contact details so that the veracity of the warrant may be checked

6.9 Interception warrants may be modified under the provisions of section 10. They 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 unless it is endorsed by the Secretary of State's personal signature. Otherwise the modification expires upon the expiry date of the warrant.

Renewal of 8(4) warrants

6.10 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 6.3 above. In particular, the applicant must 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 the section 5(3) purposes.

6.11 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 was issued on serious crime grounds, the renewed warrant is valid for a further three months, where it was issued on national security or economic well-being grounds the renewed warrant is valid for six months.

Records

6.12 A record, which shall be available for scrutiny by the Interception Commissioner, should be retained of:

- all applications made for warrants complying with section 8(4), for the renewal of such warrants, or for the modification of warrants or certificates, including the matters listed in paragraph 6.
- the signed originals of all warrants and certificates, and 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 factors by which intercepted material is selected to be read, looked at or listened to, as set out in the safeguards required by section 15 of the Act.

7. DISCLOSURE TO ENSURE FAIRNESS IN CRIMINAL PROCEEDINGS

7.1 Section 14(2) 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 14(4) specifies the authorised purposes for which retention is allowed.

7.2 This part of the Code applies to the handling of intercepted material for the purpose authorised by section 14(4)(d) of the Act, where retention is necessary to ensure that a person conducting a criminal prosecution has the information he needs to discharge his duty of ensuring the fairness of the prosecution.

7.3 The term "intercepted material" is used throughout to embrace copies, extracts or summaries made from the intercepted material as well as the intercepted material itself.

Exclusion of matters from legal proceedings

7.4 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 16 of the Act, which excludes evidence, questioning or assertion in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under the Act (or the Interception of Communications Act 1985).

7.5 Section 17 contains a number of tightly-drawn exceptions to this rule. This part of the Code deals only with the exceptions in subsections (7) to (11).

Disclosure to prosecutor

7.6 Subsection (7)(a) provides that intercepted material obtained by means of a warrant and which continues to be available, may be disclosed to a person conducting a criminal prosecution.

7.7 This may only be done for the purpose of enabling him to determine what is required of him by his duty to secure the fairness of the prosecution. The prosecutor does not have general access to the material to enable him to mount a cross-examination, or to test the defence case.

7.8 The exception does not mean that intercepted material should be retained against the mere possibility that it might be relevant to future proceedings. These rules 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*, it is probable that much material intercepted for this purpose will not survive to the

prosecution stage, as it will have been destroyed in accordance with the section 14(3) safeguards[14].

7.9 But section 17(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.

7.10 If intercepted material does continue to be available at the prosecution stage, the prosecutor should be informed that a warrant has been issued under section 5 and that material of possible relevance to the case had been intercepted. In order to discharge effectively his duty to ensure a fair prosecution, the prosecutor will be asked to assess the material's potential relevance to issues in the case. The relevant tests given in the Criminal Procedure and Investigations Act 1996, namely whether the material might undermine the case for the prosecution against the accused, or might assist the accused's defence, should be applied – although that Act strictly has no bearing on the treatment of intercepted material.

7.11 The prosecutor, having had access to the material, may conclude that the material affects, or might reasonably affect, issues in the trial. In these circumstances, he will decide how the prosecution, if it proceeds, should be presented.

Disclosure to judge

7.12 Section 17(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 gives the judge access to intercepted material, where there are exceptional circumstances making that disclosure essential in the interests of justice.

7.13 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 16(1), 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 on a fair and informed basis.

7.14 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 16(1), it must not reveal the fact of interception. This is likely to be a very

[14] **Guidance note:** The judgment of the House of Lords in *Reg. v. Preston (Stephen)* [1994] 2 AC 130 (confirmed in *Morgans v. DPP* [2000] 2 WLR 386) and the Decision of the European Commission of Human Rights (First Chamber) in *Stephen and Zena Preston v. UK* (application No. 24193/94, decision dated 2 July 1997) have both approved this practice, confirming that it preserves "equality of arms".

unusual step. The Act only allows it where the judge considers it essential in the interests of justice.

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

8. SAFEGUARDS

8.1 All material (including related communications data) intercepted under the authority of a warrant complying with section 8(1) or section 8(4) of the Act must be handled in accordance with safeguards which the Secretary of State has approved in conformity with the duty laid upon him by the Act. Approved safeguards may vary for different intercepting agencies and/or different classes of interception. The safeguards are necessarily classified and their details cannot therefore be reproduced here. All safeguards must however meet the requirements of section 14 of the Act. These requirements are set out below. In addition, the safeguards in paragraph 15 apply to warrants complying with section 8(4).

8.2 The section 14 safeguards must limit disclosure, copying and retention of material to the minimum necessary for the authorised purposes. These are defined in subsection (4) to be:

- if the action 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 well-being of the United Kingdom, or for the purpose of giving effect to the provisions of any international mutual assistance agreement.
- if the action is necessary for facilitating the carrying out of the functions of the Secretary of State under Part I, Chapter I of the Act.
- if the action is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or the Tribunal.
- if the action 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 action is necessary for the performance of any duty imposed by the Public Record Acts.

Safeguards

8.3 Section 15 provides for additional safeguards in relation to material gathered under 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.

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

Disclosure

8.4 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. 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 a required security clearance (see below), but also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties are such that he/she needs to know about the material to carry out his/her 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 must be disclosed.

8.5 The obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed. In many cases this is 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

8.6 Intercepted material may only be copied to the extent necessary for the authorised purposes. 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 records of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries, such as recording their making, distribution and (see below) destruction. Passing a copy to another person counts as disclosure – see above.

Storage

8.7 Intercepted material, and all copies, extracts and summaries of it or of communications data, 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 not cleared to see it.

Destruction

8.8 Intercepted material, and all copies, extracts and summaries of it or of communications data, must be 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.

Personnel security

8.9 Each intercepting agency maintains a list of persons who need to have access to intercepted material or communications data. All such persons must be appropriately vetted. Any person no longer needing access to perform his/her duties should be removed at once from the 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 II

9. ACCESSING COMMUNICATIONS DATA

Purposes for which communications data may be sought

9.1 Under section 21(2), communications data may be sought if it is believed to be necessary for one or more of the following purposes:

- in the interests of national security.
- for the purpose of preventing or detecting crime or of preventing disorder.
- in the interests of the economic well-being of the United Kingdom.
- in the interests of public safety.
- for the purpose of protecting public health.
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.
- for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

Public authorities permitted to access communications data under the Act

9.2 The following (described in the Act as "public authorities") are permitted under section 24(1) to grant authorisations or serve notices under Part I, Chapter II in order to access communications data:

- any police force
- the National Criminal Intelligence Service
- the National Crime Squad
- HM Customs and Excise
- the Security Service
- the Secret Intelligence Service (SIS)
- the Government Communications Headquarters (GCHQ)

The Act permits the Secretary of State to add further public authorities to this list by means of an Order before Parliament under the affirmative resolution procedure.

The appropriate level of official within each public authority for granting of authorisations or authorising notices is a minimum of Superintendent or equivalent (subject to confirmation by order under section 24(2)).

Notices and authorisations

9.3 The Act permits two different ways of accessing communications data; by a notice under section 20(4) and through an authorisation under section 20(3). A notice requires the holder of the data to collect or retrieve the data and provide

it to the public authority which served the notice, an authorisation would allow the public authority to collect or retrieve the data itself.

9.4 An authorisation should only be applied for where the postal or telecommunications operator is not capable or collecting or retrieving the communications data, or where the authorising officer has reason to believe that the particular circumstances of the case mean that accessing the data by a notice would not be possible or that accessing it in this way would be likely to prejudice the investigation.

Application – notices

9.5 The authorising officer will make a decision whether to authorise a notice based upon the application which is made. The application form is not served upon the holder of communications data, the notice which they receive contains only enough information to allow them to fulfil their duties under the Act. But the application form is subject to inspection by the Commissioner and both applicant and authorising officer may be required to justify their decisions. Applications for notices should be made on a standard form (paper or electronic) which must be retained by the public authority and which should contain the following minimum information:

- Name of officer requiring communications data.
- The operation and person to which the required data relates.
- A description, in as much detail as possible, of the communications data required.
- The reason why the specified data is considered to be necessary for one of the purposes given above.
- A consideration of the proportionality implications and a justification of why access to the material constitutes a proportionate response to the threat posed.
- A consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified. In particular where the communications data in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.
- A consideration of why the required material cannot be achieved by other less intrusive means.
- The timescale within which the communications data is required. Where the timescale within which the material is required is any greater than “routine”, the reasoning for this to be included.
- The manner in which the material should be disclosed, unless there are standard arrangements already in place.

Considerations for authorising officer

9.6 The authorising officer must make a consideration of each of the following points, and record their considerations on the application form so that he or she is in a position to justify decisions made;

- Whether the matter under investigation justifies the accessing of communications data for one of the purposes listed at section 21(2).
- Why the data is necessary for the investigation to progress.
- Why the required material cannot be gathered by other, less intrusive means.
- Where accessing the communications data is likely to result in collateral intrusion, and particularly where the communications data in question might affect religious, medical or journalistic confidentiality or legal privilege, whether the circumstances of the case still justify that access.
- Whether the required timescale is realistic and justified.

Content of notice

9.7 The notice served upon the holder of the communications data should be in a standard format and should contain the following information:

- Name, office, rank or position of authorising officer.
- Description of the required communications data.
- For which of the section 20(4) purposes the data is required.
- The manner in which the data should be disclosed.
- Contact details so that the veracity of the notice may be checked.

[copy of notice to be annexed to finalised Code following consultation]

Application – authorisation

9.8 The authorising officer will make a decision whether to grant an authorisation based upon the application which is made. The application form is subject to inspection by the Commissioner and both applicant and authorising officer may be required to justify their decisions. Applications for authorisations should be made on a standard form (paper or electronic) which must be retained by the public authority and which should contain the following minimum information:

- Name of officer requiring communications data.
- The operation and person to which the required data relates.
- A description, in as much detail as possible, of the communications data required.
- The reason why the specified data is considered to be necessary for one of the purposes given above.
- Why the applying officer believes that the communications data cannot be accessed through a 20(4) notice.
- An assessment of the practical feasibility of accessing the communications data in this way.
- A consideration of the proportionality implications and a justification of why access to the material constitutes a proportionate response to the threat posed.
- A consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified. In particular where the

communications data in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.

- A consideration of why the required material cannot be achieved by other less intrusive means.

Considerations for authorising officer

9.9 The authorising officer must make a consideration of each of the following points, and record their considerations on the application form so that he or she is in a position to justify decisions made;

- Whether the matter under investigation justifies the accessing of communications data for one of the purposes listed at section 21(2).
- Why the data is necessary for the investigation to progress.
- Why the required material cannot be gathered by other, less intrusive means.
- The reasons for believing that the particular circumstances of the case mean that accessing the data by a notice would not be possible or that accessing it in this way would be likely to prejudice the investigation.
- Where accessing the communications data is likely to result in collateral intrusion, and particularly where the communications data in question might affect religious, medical or journalistic confidentiality or legal privilege, whether the circumstances of the case still justify that access.

10. OVERSIGHT

10.1 Under the Act the Prime Minister appoints an Interception of Communications Commissioner who provides independent oversight of:

- the use by the Secretary of State of his/her powers to authorise the interception of communications.
- the performance of the duties imposed on the Secretary of State by sections 1 to 11.
- the use by relevant authorities of their powers to authorise the obtaining of communications data, and their performance of the duties imposed on them by Chapter II of Part I.
- the adequacy of the safeguards required under sections 14 and 15 of the Act, which regulate the use, disclosure, copying and retention of intercepted material and, in the case of 8(4) warrants, the examination of the material intercepted.

The Commissioner makes an annual report to the Prime Minister, which is laid before Parliament and published.[15]

10.2 The Commissioner makes regular visits to the Secretary of State, the intercepting agencies (who are acting under the authority of warrants issued by the Secretary of State) and to relevant Government departments, and carries out inspections to ensure that interceptions are authorised and carried out in accordance with the Act. The Act gives the Commissioner wide-ranging powers to require the production of documents and information. All persons involved in interception have a duty to comply with any request for information from or on behalf of the Commissioner. If the Commissioner finds any contravention of the provisions of the Act (not already reported on by the Tribunal – see below), or determines that any safeguards are inadequate, he or she will report this to the Prime Minister.

[15] **Guidance note:** The Prime Minister may, after consultation with the Commissioner, exclude from the report to be laid before Parliament any matter inclusion of which appears to him to be contrary to the public interest or which would otherwise be prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the UK, or the continued discharge of the functions of any public authority who activities are subject to review by the Commissioner.

11. COMPLAINTS

11.1 The Act establishes an independent Tribunal, which is made up of senior members of the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

11.2 The Tribunal has jurisdiction (among other things)[16]:

- to hear any proceedings against public authorities under section 7 of the Human Rights Act 1998, for actions incompatible with Convention rights in connection with the interception of communications or the obtaining of communications data;

- to investigate complaints by any persons about the interception of communications to or from those persons, or the obtaining of communications data relating to them[17].

11.3 A wide variety of persons, including all members of the intelligence agencies, all employees of police forces, and those who have provided assistance with giving effect to an interception warrant, are under a duty to provide to the Tribunal all such documents and information as the Tribunal may require in order to perform its functions.

11.4 The Tribunal may, if it wishes, seek the Commissioner's assistance in investigating any case, or otherwise seek the Commissioner's assistance or opinion for the purposes of its consideration or determination of any matter. The Commissioner is obliged to assist the Tribunal. The Tribunal is obliged to keep the Commissioner informed of the progress of any matter within the Commissioner's remit.

11.5 The Tribunal may entertain proceedings or investigate a complaint relating to interception if either

- the proceedings allege or the complaint concerns interception carried out by one of the intelligence services or those acting on their behalf, or
- the interception was carried out in 'challengeable circumstances'.

11.6 An interception is carried out in challengeable circumstances if it was carried out under the authority, or purported authority, of an interception warrant or authorisation to obtain communications data under the Act; or if it should not have been carried out without such authority, or at least without the need for authority having been properly considered.

[16] **Guidance note:** These other things include considering references by those who believe they have suffered detriment as a consequence of the prohibition on the use of material intercepted under warrant in civil proceedings. The Tribunal may also hear other civil claims related to interception or to any conduct by the intelligence agencies when the Secretary of State makes the necessary provisions.

[17] **Guidance note:** Any person may make a complaint to the Tribunal; the complainant does not need to be the person named or described in the interception warrant.

11.7 Unlawful interception by persons outside the intercepting agencies is a matter for the police to investigate.

11.8 The Tribunal, unless it believes it to be equitable in the light of all the circumstances, will not consider a complaint relating to events more than a year before the complaint is made.

11.9 When the Tribunal hears proceedings brought under section 7 of the Human Rights Act (actions incompatible with Convention rights in connection with the interception of communications or the obtaining of communications data), it will apply the same principles for determining the proceedings as would be applied by a court on an application for judicial review.

11.10 Where the Tribunal investigates a complaint by any person about the interception of communications to or from that person, or the obtaining of communications data relating to that person, the Tribunal is required to investigate whether those about whom the complaint has been made have, as a matter of fact, engaged in such conduct, and if so the authority (if any) under which they did so. In relation to these investigations the Tribunal will apply the same principles for determining the proceedings as would be applied by a court on an application for judicial review.

11.11 Where it appears to the Tribunal that any proceedings or complaint is frivolous or vexatious, it is under no duty to hear, consider or determine it.

11.12 When the Tribunal concludes its investigation of a case, it will inform the complainant either that it has made a determination in his favour, or that no determination has been made in his favour. In the former case the Tribunal may make an award of compensation or other order (including one quashing a warrant or authorisation under the Act, or requiring the destruction of relevant records). In certain circumstances the Tribunal is required to report to the Prime Minister.

11.13 If the Tribunal does not make a determination in the complainant's favour, there will be no confirmation as to whether the conduct complained of has or has not, as a matter of fact, taken place, nor as to the existence of any warrant or authorisation relating to the complainant.

11.14 There is no appeal against the decision of the Tribunal in respect of proceedings brought under section 7 of the Human Rights Act, or of complaints about the interception of communications or the obtaining of communications data.

[How to make a complaint – directions to published leaflets and/or websites, complaints forms.]