Home Office

Interception of Communications

Pursuant to Schedule 7 to the Investigatory Powers Act

[Autumn 2016]

DRAFT Code of Practice

Contents

1. Introduction

1.1. This Code of Practice relates to the powers and duties conferred or imposed under Part 2 and Chapter 1 of Part 6 of the Investigatory Powers Act 2016 ("the Act"). It provides guidance on the procedures that must be followed when interception of communications can take place under these provisions. This Code of Practice is primarily intended for use by those public authorities listed in section 18 of the Act. It will also allow postal and telecommunication service operators and other interested bodies to understand the procedures to be followed by those public authorities.

1.2. The Act provides that all codes of practice issued under Schedule 7 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 Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and capabilities conferred by the Act on the intercepting agencies, it must be taken into account.

1.3. For the avoidance of doubt, the guidance in this code takes precedence over any contrary content of an intercepting agency's internal advice or guidance.

2. Scope and definitions

What is interception?

2.1 Section 4 of the Act states that a person intercepts a communication in the course of its transmission by means of a telecommunication system if they perform a relevant act in relation to the system and the effect of that act is to make any content of the communication available at a relevant time to a person who is not the sender or intended recipient of the communication. The interception may require the assistance of a communications service provider, and more information on this is provided at Chapter 7. Section 4(2) sets out that "relevant act" in this context means:

- Modifying, or interfering with, the system or its operation;
- Monitoring transmissions made by means of the system;
- Monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system

What is a communications service provider?

2.2 Throughout this code, communications service provider is used to refer to a telecommunications operator or postal operator. Communications service provider is not a term used in the Act.

2.3 A telecommunications operator is a person who offers or provides a telecommunication service to persons in the UK or who controls or provides a telecommunication system which is, (in whole or in part) in or controlled from the UK. A postal operator is a person providing a postal service to a person in the UK. These definitions make clear that obligations in the Parts of the Act to which this code apply cannot be imposed on communications service providers whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK.

2.4 Section 237(11) of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the telecommunications service provider); and defines 'telecommunications system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. The definition of 'telecommunications service' in the Act is intentionally broad so that it remains relevant for new technologies.

2.5 The Act makes clear that any service which consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunications system is included within the meaning of 'telecommunications service'. Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.

2.6 The definition of a telecommunications operator also includes application and website providers but only insofar as they provide a telecommunication service. For example an online market place may only be a telecommunications operator as it provides a connection to an application/website. It may also be a telecommunications operator if and in so far as it provides a messaging service.

2.7 Telecommunications operators may also include those persons who provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in commercial premises such as hotels or public premises such as airport lounges or public transport.

2.8 In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider, or where there are security implications in doing so, the data may be sought from the communications service provider which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of communications data for example, where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room.

2.9 Section 238(7) of the Act defines 'postal service' to mean any service which consists in one or more of the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items and which is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to transmit postal items from place to place.

2.10 For the purposes of the Act a postal item includes letters, postcards and their equivalents as well as packets and parcels. It does not include freight items such as containers. A service which solely carries freight is not considered to be a postal service under the Act. Where a service carries both freight and postal items it is only considered to be a postal service in respect of the transmission of postal items.

What is meant by the content of a communication?

2.11 The content of a communication is defined in section 237(6) of the Act as the data which reveals anything of what might be reasonably be considered to be the meaning (if any) of that communication.

2.12 When one person sends a message to another what they say or what they type in the subject line or body of an email is the content. However there are many ways to communicate and the definition covers the whole range of telecommunications. What is consistent is that the content will always be the part of the communication (whether it be the speech of a phone call or the text of an email) that conveys the substance or meaning of the sender is intending to convey to the recipient. It is that meaning that the Act defines as content.

2.13 When a communication is sent over the telecommunication systems it can be carried by multiple providers. Each provider may need a different set of data in order to route the communication to its eventual destination. The definition of content ensures that the elements of a communication which are considered to be content do not change depending on which communication provider is carrying the communication.

2.14 There are two exceptions to the definition of content set out in section 237(6). The first is there to address inferred meaning. When a communication is sent, the simple fact of the communication conveys some meaning, e.g. it can provide a link between persons or between a person and a service. This exception makes clear than any communications data associated with the communication remains communications data and the fact that some meaning can be inferred from it does not make it content.

2.15 The second makes clear that systems data cannot be content. In practice this means that an intercepting authority should first determine whether the data enables or otherwise facilitates the functioning of a system or service. If the answer to this question is yes, then the data is systems data regardless of whether it may reveal anything of what might be reasonably be considered to be the meaning (if any) of the communication[1].

Postal definitions

2.16 In the postal context anything included inside a postal item, which is in transmission, will be content. Any message written on the outside of a postal item, which is in transmission, may be content and fall within the scope of the provisions for interception of communications. For example, a message written by the sender for the recipient will be content but a message written by a postal worker concerning the delivery of the postal item will not.

What is meant by postal data?

2.17 Postal data is defined in section 238(4) of the Act and includes specified categories of data written on the outside of a postal item. Any message written on the outside of a postal item, which is in transmission, may be content and fall within the scope of the provisions for interception of communications. For example, a message written by the sender for the recipient will be content but a message written by a postal worker concerning the delivery of the postal item will not. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is postal data.

[1] When permitted by the Act, certain identifying data may also be separated from the remainder of a communication in circumstances where, if it were so separated, it would not reveal anything of what might reasonably be considered to be the meaning of the communication. Identifying data and systems data may be obtained by interception or equipment data warrants under Parts 2, 5 and Chapters 1 and 3 of Part 6 of the Act.

3. Unlawful interception – criminal and civil offences

3.1 Interception is lawful only in the limited circumstances set out in section 6 of the Act. This includes when it is carried out in accordance with a warrant issued under Part 2 or Chapter 1 of Part 6 of the Act, or under another statutory power exercised for the purpose of obtaining stored communications (on which further detail is provided at Chapter 12 of this Code). Interception can also be lawful in other proscribed circumstances which are set out in sections 42 to 50 of the Act (on which further detail is provided in Chapter 12 of this Code) such as with the consent of the sender and recipient of the communication or within prisons.

3.2 Section 3(1) of the Act makes it a criminal offence for a person intentionally, and without lawful authority, to intercept in the UK any communication in the course of its transmission if that communication is sent via a public or private telecommunication system or a public postal service.

3.3 Section 3(2) of the Act states that it is not a criminal offence for a person to intercept a communication in the course of its transmission by means of a private telecommunication system if the person who carries out the interception has a right to control the operation or use of the system or has the express or implied consent of the controller. An example may be where a company monitors communications over its computer systems in the workplace.

3.4 The penalty for unlawful interception is up to two years' imprisonment or an unlimited fine.

3.5 Section 7 of the Act enables the Investigatory Powers Commissioner to serve a monetary penalty notice imposing a fine of up to £50,000 if he or she is satisfied that:

- A person has not committed an offence under section 3(1) of the Act.
- But, that person has intercepted a communication at a place in the UK without an appropriate authorisation under the Act being in place;
- The communication was intercepted in the course of its transmission by means of a public telecommunication system; and
- The person was not, at the time of the interception, making an attempt to act in accordance with an interception warrant which might explain the interception;

3.6 Guidance on the administration of these sanctions is available on the Investigatory Powers Commissioner's website.

3.7 Section 8 of the Act provides a civil right of redress for the sender or intended recipient of a communication. The cause of action arises where a communication is intercepted, without lawful authority, in the course of its transmission by means of a private telecommunication system or by means of a public telecommunication system to or from apparatus that is part of a private telecommunication system by or on behalf of the person with the right to control the operation or use of the private telecommunications system.

4. Warranted interception – general rules

4.1 Interception has lawful authority where it takes place in accordance with a warrant issued under Part 2 or Chapter 1 of Part 6 of the Act. Chapter 12 of this Code deals with the circumstances in which interception is permitted without a warrant.

4.2 Section 15(2) of the Act makes clear that a targeted interception warrant may authorise the obtaining of secondary data. Obtaining secondary data may be the sole purpose of the warrant or may be authorised in addition to the interception of the communications described in the warrant. Section 16(6) of the Act defines secondary data in relation to a targeted interception warrant as being data which is obtained directly as a consequence of the execution of an interception warrant. Sections 128(4) and 128(5) of the Act define secondary data in relation to a bulk interception warrant; this definition also includes technical information that enables the telecommunications systems or services to function but does not relate to the sender or recipient of any communication.

4.3 Section 4 of the Act also applies to interception in relation to postal services. Section 4 (7) confirms that, for the purpose of determining whether a postal item is in the course of transmission by means of a postal service, section 125(3) of the Postal Services Act 2000 applies. The Act provides that a postal packet is in the course of transmission by post from the moment it is delivered to any post office or post office letter box to the time of being delivered to the addressee. Chapter 2 provides more information on postal data.

Types of interception warrant

4.4 The Act provides for four types of warrant which may authorise interception and examination with a warrant. Guidance on targeted warrants provided for in Part 2 of the Act is set out in Chapter 5 of this Code. Guidance on bulk warrants provided for in Part 6 is set out in Chapter 6 of this Code.

- A **targeted interception warrant** issued under section 15(1)(a) of the Act authorises or requires the person to whom it is addressed to intercept the communications described in the warrant and/or obtain secondary data. A targeted interception warrant must specify a particular person, premises or operation. Section 17 of the Act also makes clear that a warrant may relate to more than one person or set of premises in certain circumstances: where a group of person share a common purpose or carry on a particularly activity; where the conduct authorised or required by the warrant is for the same investigation or purpose; for testing apparatus, systems or other capabilities; or for training purposes. This type of targeted interception warrant is sometimes referred to as a “thematic warrant” and more detail is provided at paragraph 5.15.

- A **targeted examination warrant** issued under section 15(1)(b) of the Act authorises the person to whom it is addressed to select for examination intercepted content obtained under a bulk interception warrant. This type of warrant must be sought in all cases where content is to be selected for

examination on the basis of criteria referable to an individual who the person making the request believes will be in the British Islands at the time of the interception. Where an individual enters or is found to be in British islands, a senior official may authorise the continued selection of his content using only the existing criteria, for a period of up to five working days. This period allows a targeted examination warrant to be sought without losing coverage of intelligence targets.

- A **mutual assistance warrant** issued under section 15(1)(c) of the Act authorises or requires the person to whom it is addressed (an EU or International authority for the purposes of a specified international treaty) to give assistance in relation to the intelligence request specified in the warrant.

- A **bulk interception warrant** issued under section 128 of the Act is a warrant which has as its main purpose the interception of overseas-related communications[2] and/or the obtaining of secondary data from such communications, and which authorises the interception of and/or obtaining of secondary data from the communications described in the warrant, as well as the selection for examination of the intercepted content or secondary data. Section 128 provides for a bulk warrant to be issued for the purpose of obtaining secondary data only. Such a warrant will also authorise any conduct it is necessary to undertake to do what is authorised by the warrant. This may include the interception of the content of communications but this is only permitted in so far as it is necessary in order to obtain the secondary data from the communications described in the warrant. In the event that any content is intercepted under a secondary data only warrant, the intercepted content must not be selected for examination.

Necessity and proportionality

4.5 Interception of communications will almost always involve an interference with an individual's rights under Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR). This would only be justifiable if the interception is necessary for a legitimate purpose and proportionate to that purpose. The Act recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the following statutory grounds set out in section 20 of the Act:

- In the interests of national security;

- For the purpose of preventing or detecting serious crime; serious crime is defined in section 239(1) as crime that comprises an offence for which a person who has reached the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

[2] Section 128(3) sets out that, within the chapter on bulk interception, "overseas-related communications" means communications sent or received by individuals who are outside the British Islands

- In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security. The power to issue an interception warrant for the purpose of safeguarding the economic well-being of the UK may only be exercised where it appears to the Secretary of State and Judicial Commissioner that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant on these grounds if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant for the purpose of safeguarding the economic well-being of the UK should therefore identify the circumstances that are relevant to the interests of national security. The power to issue an interception warrant for the purpose of safeguarding the economic well-being of the UK may also only be exercised in circumstances where the information it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.
- For the purpose of giving effect to the provisions of an EU mutual assistance instrument or an international mutual assistance warrant. More information on mutual assistance warrants is provided at paragraph 5.10 of this document.

4.6 The Secretary of State must also believe that the interception is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate.

4.7 In the case of warrants issued under section 17(2)(c) of the Act for the purposes of testing and training, proportionality should be considered by assessing the potential for, and seriousness of, intrusion into any affected persons' privacy against the benefits of carrying out the proposed testing or training exercise.

Is the investigatory power under consideration appropriate in the specific circumstances?

4.8 No interference with privacy should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

4.9 The following elements of proportionality should therefore be considered:

- Balancing the extent of the proposed interference with privacy against what is sought to be achieved;
- Explaining how and why the methods to be adopted will cause the least possible interference on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result.

- Explaining, as appropriate, what other methods have been considered and were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the use of the proposed investigatory power.

Trade Unions

4.10 As set out in clauses 20 (and 21), the fact that the information that would be obtained under the a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State (or Scottish Ministers). Intercepting authorities are permitted to apply for a warrant against members or officials of a trade union considered to be a legitimate intelligence target where that is necessary for one or more of the statutory purposes, so long as the interception is proportionate to what is sought to be achieved.

The intercepting authorities

4.11 There are a limited number of persons who can make an application for an interception warrant, or for whom an application can be made on their behalf as set out at section 16. These are:

- The Director General of the Security Service.
- The Chief of the Secret Intelligence Service.
- The Director of the Government Communications Headquarters (GCHQ).
- The Director General of the National Crime Agency (NCA handles interception on behalf of law enforcement bodies in England and Wales).
- The Commissioner of the Police of the Metropolis (the Metropolitan Police Counter Terrorism Command handles interception on behalf of Counter Terrorism Units, Special Branches and some police force specialist units in England and Wales).
- The Chief Constable of the Police Service of Northern Ireland.
- The Chief Constable of the Police Service of Scotland.
- The Commissioners for Her Majesty's Revenue & Customs (HMRC).
- The Chief of Defence Intelligence.
- A person who is the competent authority of a country or territory outside the UK for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.

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

4.13 In the case of bulk interception warrants, the only persons who can make an application, or on whose behalf an application can be made, are:

- The Director General of the Security Service.

- The Chief of the Secret Intelligence Service.
- The Director of the Government Communications Headquarters (GCHQ).

4.14 All interception warrants are issued by the Secretary of State. Even where the urgency procedure is followed, the Secretary of State personally authorises the warrant, although the warrant itself is signed by a senior official. More detail on the urgency procedure is set out at paragraph 5.64.

5. Targeted interception warrants

5.1 This section applies to the three kinds of warrants that may be issued under Part 2 of the Act for the purpose of targeted interception and examination with a warrant (as set out at paragraph 4.4). These are:

- Targeted interception warrants;
- Targeted examination warrants (authorising the selection for examination of intercepted content obtained under a bulk interception warrant)
- Mutual assistance warrants.

5.2 Responsibility for the issuing of interception warrants rests with the Secretary of State. The role of the Judicial Commissioner in authorising warrants is explained in paragraph 5.59. Interception and examination warrants, when issued, are addressed to the person who submitted the application. A copy may then be served on any person who may be able to provide assistance in giving effect to that warrant. Prior to submission to the Secretary of State and Judicial Commissioner, each application should be subject to a review within the agency seeking the warrant. This review involves scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 20 of the Act and whether the interception proposed is both necessary and proportionate. A copy of each warrant application should be retained by the intercepting agency.

5.3 In no circumstances may a UK intercepting agency seek to circumvent the requirement to obtain a warrant by asking an international partner to undertake interception on its behalf. Paragraph 5.50 provides further information on mutual assistance warrants.

Reviewing warrants

5.4 Regular reviews of all warrants should be undertaken during their currency to assess the need for the interception activity to continue. Particular attention should be given to the need to review warrants frequently where the interception involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

5.5 In each case, unless specified by the Secretary of State or Judicial Commissioner, the frequency of reviews should be determined by the intercepting agency who made the application. This should be as frequently as is considered necessary and proportionate.

5.6 In the event that there are any significant and substantive changes to the nature of the interception during the currency of the warrant, the intercepting agency should consider whether it is necessary to apply for a new warrant.

Format of warrant applications

Targeted interception warrants

5.7 An application for a targeted interception warrant should contain the following information:

a) The background to the operation or investigation in the context of which the warrant is sought;

b) A warrant that relates to a particular person or organisation or to a single set of premises must name or describe that person or organisation or those premises.

c) A warrant that relates to a group of persons who share a common purpose or who carry on (or who may carry on) a particular activity must describe that purpose or activity, and name or describe as many of those persons as it is reasonably practicable to name or describe.

d) Where the conduct authorised or required by the warrant relates to more than one person or organisation or more than one set of premises, and where the warrant is for the purposes of a single investigation or operation it should describe the investigation or operation and name or describe as many of those persons or organisations, or as many of those sets of premises as it is reasonably practicable to name or describe.

e) A warrant that relates to any testing or training activities must describe those activities and name or describe as many of the persons whose communications will or may be intercepted as it is reasonably practicable to name or describe.

f) A description of the communications to be intercepted or the secondary data to be obtained, details of the communications service provider (s) and an assessment of the feasibility of the interception to the extent known at the time of the application;[3]

g) A description of the conduct to be authorised or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant. This conduct may include the interception of other communications not specifically identified by the warrant; it may also include conduct for obtaining secondary data from communications

h) An explanation of why the interception warrant is considered to be necessary on one or more of the grounds set out in section 20;

i) Consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, including, where appropriate, explaining why less intrusive alternatives have not been or would not be as effective;

j) Consideration of any collateral intrusion and why that intrusion is justified in the circumstances;

[3] This assessment is normally based upon information provided by the relevant communications service provider. Where a warrant identifies the communications to be intercepted by reference to a number, apparatus or other factors, the warrant authorises the interception of those communications by all associated numbers, apparatus or factors. For example, where a mobile phone number is specified, that includes not only the phone number given to the user, but also any number or address used to identify that phone or handset to the network or communications service provider. Such a number or address may be temporary or permanent

k) Whether the warrant is likely or intended to result in the obtaining of privileged or other confidential material or whether the purpose of the warrant is to obtain a Member of Parliament's communications (see Chapter 9), and if so what protections it is proposed will be applied to the handling of the information so obtained;

l) Where an application is urgent, the supporting justification;

m) An assurance that all the material obtained under the warrant will be kept for no longer than necessary and handled in accordance with the safeguards required by section 51 of the Act (see chapter 9).

Targeted examination warrants

5.8 A targeted examination warrant described in section 15(3) of the Act authorises the person to whom it is addressed to carry out the selection for examination, in breach of the prohibition in section 143(4) of the Act, of intercepted content obtained under a bulk interception warrant of an individual known for the time being to be in the British Islands.

5.9 Targeted examination warrants must be issued by the Secretary of State on an application by or on behalf of the head of an Intelligence Service. An application for a targeted examination warrant should contain:

a) The background to the operation or investigation in the context of which the warrant is sought;

b) Where the warrant relates to a particular person or organisation or to a single set of premises, a name or description of that person or organisation or those premises;

c) Where a warrant relates to a group of individuals who share a common purpose or who carry on (or may carry on) a particular activity, a name or description of that purpose or activity, and of as many of those individuals as it is reasonably practicable to name or describe

d) Where a warrant relates to more than one person or organisation, or more than one set of premises for the purposes of a single investigation or operation, a description of the investigation or operation and a name or description of as many of those persons or organisations, or sets of premises as it is reasonably practicable to name or describe.

e)

f) Where a warrant that relates to any testing or training activities, a description of those activities and a name or description of as many of the individuals whose communications content will or may be selected for examination as it is reasonably practicable to name or describe

g) A description of the relevant content that is to be selected for examination[4].

Where a warrant identifies the relevant content to be selected for examination by reference to a number, apparatus or other factors, the warrant authorises the selection of that content by all associated numbers, apparatus or factors. For example, where a mobile phone number is specified, that includes not only the phone number given to the user, but also any number or address used to identify that phone or handset to the network or CSP communications service provider (for example the International Mobile Subscriber Number (IMSI). Such a number or address may be temporary or permanent.[5] See Schedule 1 to the Interpretation Act 1978.

h) An explanation of why the selection for examination is considered to be necessary under the provisions of section 20;

i) Consideration of why the selection for examination to be authorised by the warrant is proportionate to what is sought to be achieved, including, where appropriate, explaining why less intrusive alternatives have not been or would not be as effective;

j) Consideration of any collateral intrusion and why that intrusion is justified in the circumstances;

k) Whether the warrant is likely or intended to result in the obtaining of privileged or other confidential material or whether the purpose of the warrant is to obtain a Member of Parliament's communications and if so, what protections it is proposed will be applied to the handling of the material so obtained;

l) Where an application is urgent, the supporting justification;

m) An assurance that any content selected will be kept for no longer than necessary and handled in accordance with the safeguards required by section 51 of the Act (see chapter 9).

Mutual Assistance Warrants

5.10 In addition to the information at paragraph 5.7 above which apply equally to mutual assistance warrants, section 38(1) contains additional requirements in relation to a subset of such mutual assistance warrants. Such warrants must contain whichever of the following statements is applicable:

- A statement that the interception subject (defined as the person, group of persons or organisation about whose communications information is sought by the interception to which the warrant relates) appears to be outside the United Kingdom

- A statement that the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom

Subject-matter and scope of targeted warrants

5.11 Targeted warrants authorise or require the interception of communications or the obtaining of secondary data described in the warrant, or the selection for examination of relevant content intercepted under a bulk interception warrant. The warrant must specify the factors used for identifying the communications to be intercepted or selected for examination (see section 29(8) and (9)).

5.12 Section 17 sets out the subject-matter of targeted warrants and constrains what communications can be described in the warrant, or selected for examination. Section 17 therefore sets the "scope" of a targeted warrant. Any communications may technically be intercepted or selected by the warrant, provided they fall within its scope. The subject-matter of interception and examination warrants may be targeted (a single person or organisation) (section 17(1)) or thematic targeted (section 17(2)).

1. Targeted warrants relating to a person, organisation or set of premises

5.13 In many cases, interception and examination warrants will relate to subjects as set out in 17(1). Section 17(1) warrants must relate to a particular person, organisation or a single set of premises. A "person" for these purposes may be an individual but, as defined in the Interpretation Act 1978, a "person" includes a body of persons corporate or unincorporated. [5] An "organisation" may include entities that are not legal persons. This means, for example, that a warrant may relate to a particular company. In such a case the company is the "person" to which the warrant relates and section 29(3) will not impose an obligation to name individual employees or workers in the warrant. There will be no intrusion into the privacy of employees unless the warrant specifies a factor that identifies their communications. Similarly, in the case of an unincorporated body such as a partnership, a warrant may refer just to the partnership, but will authorise the interception of communications sent by, or intended for, any members of the partnership.

5.14 In practice, an application for a targeted warrant of this nature falling within section 17(1) is likely to be appropriate where the purpose of the warrant is to obtain intelligence about the legal person or organisation itself, rather than the individuals within the company or organisation. Where a warrant relates to a legal person or organisation, the Act does not require the intercepting agency to name or describe individuals whose communications may be intercepted. In many cases the identities of these individuals will not be known (or could only be ascertained by further interferences with privacy). Individual names are not required to ascertain the scope of the warrant or the interference with privacy authorised.

Example 1

Intelligence suggests that a UK-based company is exporting in breach of sanctions. At this stage the intelligence interest is in the company, its plans and activities, and not those working for the company. It is not known who within the company might be involved in the illegal exporting. In order to develop this intelligence it is necessary to intercept the company's communications. It is necessary to intercept the company's office network, but this is not confined to a single premises because a number of the employees carry out mobile working, as in many modern businesses. Interception of the company's network enables coverage of the organisation's activities, including communications with overseas clients, but this network is used by a range of company staff, not just a few individuals. If the interception reveals that only a small number of individuals within the company are of intelligence interest and that interception of the company as a whole is no longer necessary and proportionate, then the warrant should be cancelled and new targeted warrants sought which focus on the individuals concerned.

[5] See Schedule 1 to the Interpretation Act 1978.

Targeted thematic warrants

5.15 In other cases, interception and examination warrants will relate to thematic subjects**.** These are sometimes referred to as targeted 'thematic' warrants. Thematic subjects are described in section 17(2) of the Act and relate to more than one particular person, organisation or premises. Section 29(4) and (5) impose certain additional requirements as to what such warrants must specify. Where a targeted thematic warrant relates to a group of persons who share a common purpose, for example, the warrant may relate to some or all of the members of a group providing it is necessary and proportionate. The warrant must name or describe as many of the persons who's communications are to be intercepted as reasonably practicable. The warrant is defined by the subject-matter that the Secretary of State has approved, and not defined by the list of persons. Anyone in the group will be within the scope of the warrant, although their privacy will not be intruded upon unless the warrant specifies a phone number etc. that identifies their communications to be intercepted. A thematic warrant can be modified to include more members of the group as it becomes necessary and proportionate to do so. Further guidance on targeted thematic warrants is set out below.

5.16 Section 17(2) of the Act sets out the types of subject that a targeted thematic warrant can relate to. These are:

a) A group of persons who share a common purpose. For example, the warrant could authorise the interception of mobile phones being used by an organised crime group engaged in trafficking drugs into the UK.

b) A group of persons who carry on, or may carry on, a particular activity. Groups who carry on a particular activity may comprise collections of people who share a common activity but have no other association with each other. For example, the warrant could relate to users of a child abuse website but who are not necessarily known to one another.

c) More than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purpose of a single investigation or operation. For example, the warrant could authorise the interception of mobile phones associated with individuals who are engaged in or supporting Islamist extremist attack planning in the UK or it could relate to an operation to understand the use of certain dark web technologies by serious criminals.

d) The testing, maintenance or development of apparatus, systems or other capabilities relating to the interception of communications in the course of their transmission by means of a telecommunication system or to the obtaining of secondary data. For example, the warrant could relate to testing a new technique against computers, in a controlled test environment, to help ensure that the technique is effective.

5.17 The Act does not limit the number of persons, organisations or sets of premises to which a thematic targeted warrant may relate. When the warrant is issued it must name or describe all of the persons, organisations or sets of premises within the scope of the thematic warrant as far as is reasonably practicable at that time. The thematic warrant application must contain as much information as possible to enable a Secretary of State to assess the scope of the warrant by reference to the group, the investigation or operation, or the testing or training activity in issue. This will ensure that the extent of the reasonably foreseeable interference with privacy caused by the interception, or selection for examination, can be properly and fully assessed by the Secretary of State. It will also ensure that the Secretary of State, and the Judicial Commissioner when considering the warrant application, can be satisfied as to the necessity and proportionality of the conduct to be authorised. This will also assist those executing the warrant so that they are clear as to the scope of the warrant.

5.18 In any case where an agency wishes to intercept, or select for examination the communications of a person who is a member of a relevant legislature, the agency must apply for a targeted warrant in respect of that person under 17(1)(a) (see Chapter 9 for further guidance on confidential information and sensitive professions).

Example 1

An IT attack has taken place on the UK banking network. One of the attackers is known; access to some of his email communications indicates that further attacks are imminent and could cripple the banking network. The known attacker has been in communication with a large number of other individual contacts who need to be rapidly triaged. A thematic warrant is requested to allow the agencies to gain insight into the individuals in contact with the attacker and identify which are linked to attack planning and should be the focus of closer investigation.

Example 2

Several people are using a communication platform to communicate covertly with each other between Syria and the UK, and then with other extremist contacts in the UK. Their identities are unknown. The communications are the only source of intelligence available on the group. A thematic warrant authorises the interception of the suspect communications. The content of those messages reveals terrorist facilitation activity, including the provision of passports and fighters. This information enables the use of other intelligence techniques to gain insights into their activities and disrupt them.

Example 3

Users of a particular child abuse website use a platform to communicate. The users could be like-minded individuals engaging in the same activity, not necessarily an organised grouping co-ordinating the abuse; it is not possible to know how many of the users are known to each other. It is known that active use of the platform is a strong signifier of criminal activity associated with child abuse. A thematic warrant is requested to allow interception of the communications of the platform and its users: this provides insight into the criminal activity, allowing the agency to identify previously-unknown offenders and providing the opportunity to investigate and disrupt them. Follow-on investigation may reveal individual identities, or computers or telephones used by those individuals, which were not previously known.

Example 4

An operation is set up to look at cybercriminals' use of dark web technology. There is a focus on one particular technology that provides a secure communications channel, and a thematic warrant is sought to authorise interception of that communications channel, to access the communications of the cybercriminals. It is not possible to know how many of the cybercriminals are known to each other, although they are using the same technology. This interception enables access to cybercriminal communications that would not otherwise be technically available. Where previously-unknown cybercriminals can be identified through these means, follow-on investigation may reveal individual identities, or computers or telephones used by those individuals, which were not previously known.

5.19 As set out at paragraph 5.4, there is an on-going duty to review the necessity and proportionality of warrants and to cancel them as necessary. This duty is especially important in respect to targeted thematic warrants given they relate to more than one person, organisation or set of premises.

5.20 Where a warrant requesting agency becomes aware of a new individual factor which relates to activity covered by a thematic warrant, such as a phone associated with a person, organisation or premises described in the warrant, and wishes to start intercepting or selecting these communications, the agency must make a minor modification to specify the factor in the warrant (in accordance with section 29(8)) that identifies those communications. This will be within the scope of the warrant if the individual, organisation or premises is within the subject matter of the original warrant. The factor can only be added if it will identify communications to or from someone who is named or described in the warrant.

5.21 Where a new person, organisation or set of premises is to be added to a targeted thematic warrant, the agency must seek a major modification from the warrant granting department, to add the name or description of the person, organisation or set of premises to the warrant in accordance with section 29(4) or (5) (see section in this code on Major Modifications). For example, if the warrant relates to a single investigation (as set out in 17(2)(b)), a person can only be added for the purpose of that investigation. In addition, section 29(4) and (5) requires that warrant that relates to a group of persons or a single investigation must name or describe as many of the persons, premises or organisations as is reasonably practicable. Complying with that duty may require a major modification. Modifying a warrant to name or describe a new person etc. is likely to be reasonably practicable in cases where, for example, an agency has sought a thematic warrant relating to members of an organised crime group involved in a kidnapping. If the agency becomes aware of a newly identified member of that group and wishes to intercept his communications, the warrant should be modified as soon as reasonably practicable to include that individual's name or description, and the factors to be used for identifying his communications. This will assist the Secretary of State or senior official authorising the modification to understand the communications that are being intercepted or selected, and will assist Judicial Commissioners' oversight of the warrant.

5.22 Section 29 does not require the agency to seek a major modification to add an individual's name or description unless it is reasonably practicable to do so. For example, it may not be reasonably practicable to make immediate modifications in a fast moving threat to life operation where it may be possible to identify communications addresses for a group, but the members cannot be accurately named or described or are changing so quickly as to make it impracticable to keep updating the warrant].

5.23 In no circumstances is it possible to modify a warrant so as to authorise conduct which does not fit within the activity authorised in the original warrant. For example, a thematic warrant targeting the communications of a group believed to be involved in a kidnapping can only be modified to include a new person who is believed to be involved in the same kidnap. Agencies may only modify a warrant to add a person, organisation or set of premises when the warrant is a thematic warrant. Warrants that relate to a particular person, organisation or set of premises under section 17(1) may not be so modified.

Combined warrants

5.24 Schedule 8 to the Act provides for combined warrants. Combining warrant applications is not mandatory, but provides the option for grouping warrant applications for the same investigation/operation together so that, the Secretary of State and/or Judicial Commissioner who is to issue the warrant can consider the full range of actions that may be undertaken in relation to the investigation. It allows a more informed decision about the necessity and proportionality of the totality of the action being undertaken and may be more efficient for the agency applying for the warrant as it reduce duplication of identical information across warrant applications.

5.25 For combinations of warrants under schedule 8, the authorisation process set out at paragraph 5.4 will apply. In some cases this will necessitate a higher authorisation process than individual warrant applications. Where one of the warrants or authorisations within a combined warrant is cancelled, the whole warrant ceases to have effect under the same procedures set out at paragraph 5.92. For example, if an operation authorised with a combined equipment interference and interception warrant no longer required interception, the whole warrant would be cancelled (and the relevant communications service provider notified if applicable) and a new equipment interference warrant sought to cover the remaining actions under the operation. Combined warrants may also be applied for on an urgent basis.

5.26 Where warrants of different durations are combined, the shortest duration should apply, except for where a combined warrant issued on the application of the head of an intelligence service and with the approval of a Judicial Commissioner includes an authorisation for directed surveillance – in this case, the duration of the warrant is six months.

5.27 The requirements that must be met before a warrant can be issued should apply to each part of a combined warrant. So, for example, where a combined warrant includes a targeted interception warrant, all the requirements that would have to be met for a targeted interception warrant to be issued should be met for the interception warrant part of the combined warrant.

5.28 The duties imposed by clause 2 (having regard to privacy) apply to combined warrants as appropriate. The considerations that apply when deciding whether to issue, renew, cancel or modify a Part 2 or 5, will apply when such a warrant forms part of a combined warrant. So the targeted interception element of a combined warrant cannot be issued without having regard to privacy in accordance with clause 2.

5.29 It is possible to serve only part of a combined warrant. For example, if a combined warrant included a targeted interception warrant and an authorisation for directed surveillance, it is possible to serve just the part of the warrant that is the targeted interception warrant.

5.30 Paragraph 20 (schedule 8) provides that various rules regarding warrants apply separately to the relevant part of a combined warrant. The duty of operators to give effect to a warrant applies separately in relation to each part of a combined warrant. So, for example, clause 41(duty of operators to assist with implementation) would apply to the targeted interception part of a combined warrant but only to that part.

5.31 Similarly, safeguards also apply to individual parts of a combined warrant. For instance, where a combined targeted interception and intrusive surveillance warrant has been issued, the safeguards that apply to a targeted interception warrant apply to the part of the combined warrant that is a targeted interception warrant. Clause 54 (duty not to make unauthorised disclosures) and 56 (the offence of making unauthorised disclosures) apply to the targeted interception part of a combined warrant.

5.32 The exclusion of matters from legal proceedings (clause 53) continues to apply to an interception warrant that is part of a combined warrant. However, when an equipment interference warrant is combined with an interception warrant the material derived from equipment interference may still be used in legal proceedings if required. If material derived from equipment interference authorised by a

combined warrant can be recognised as a product of interception, and therefore reveals the existence of a warrant issued under Chapter 1 of Part 1 of the Act, the material is excluded from use in legal proceedings according to section 53 of the Act.

5.33 Should the exclusion from legal proceedings mean that there may be difficulties in disclosing any material obtained under a combined warrant that included an interception warrant, intercepting agencies may wish to consider the possibility of seeking individual warrants instead.

Applications made by or on behalf of the intelligence services

5.34 Paragraph 1 of Schedule 8 sets out that the Secretary of State may issue a warrant that combines a targeted interception warrant with one or more of the following:

- A targeted equipment interference warrant under section 96(1)
- A targeted examination warrant under section 19(2) or section 96(3)
- A directed surveillance authorisation under section 28 RIPA
- An intrusive surveillance authorisation under section 32 RIPA
- A property interference authorisation under section 5 of the Intelligence Services Act 1994

5.35 Additionally, a targeted examination warrant under section 19(2) and targeted examination warrant under 96(3) may be combined.

5.36 The Secretary of State's decision to issue a combined warrant requires the approval of a Judicial Commissioner in the same way as the decision to issue an interception warrant. The double lock applies to combined warrant. However, where a warrant under section 5 of the Intelligence Services Act is forms of the combined warrant, paragraph 21(3) of Schedule 8 sets out that the Judicial Commissioner does not have the same role in relation to that part of the application.

Applications made by or on behalf of the Chief of the Defence Intelligence

5.37 Paragraph 2 of Schedule 8 sets out that the Secretary of State may, on an application made by or on behalf of the Chief of Defence Intelligence, issue a warrant that combines a targeted interception warrant under section 19(1) with one or more of the following:

- A targeted equipment interference warrant section 98.
- A directed surveillance authorisation under section 28 of RIPA
- An intrusive surveillance authorisation under section 32 of RIPA

Applications made by or on behalf of a relevant law enforcement interception authority

5.38 Paragraph 3 of Schedule 8 sets out that the Secretary of State may issue a warrant that combines a targeted interception warrant with one or more of the following:

- A targeted equipment interference warrant under section 100

- A property interference authorisation under section 93 of the Police Act 1997
- A directed surveillance authorisation under section 28 of RIPA
- An intrusive surveillance authorisation under section 32 of RIPA

Applications issued by Scottish Ministers

5.39 The intelligence services cannot carry out intrusive or directed surveillance under RIPSA. Consequently, the head of an intelligence service cannot apply to the Scottish Ministers for combined warrants including RIPSA authorisations.

5.40 The Scottish Ministers are able to issue warrants under section 7 of ISA in certain circumstances. These are set out in Schedule 1 to the Scotland Act 1998 (Transfer of Functions to the Scottish Ministers etc.) Order 1999. The combinations of warrants that the Scottish Ministers can issue on the application of the head of an intelligence service includes section 5 ISA warrants.

5.41 Paragraph 4 of Schedule 8 sets out that, on application by the head of an intelligence service, a Scottish Minister may issue a warrant combining a targeted interception warrant under section 19(1) with one or more of the following:

- A targeted examination warrant under section 21(2)
- A targeted equipment interference warrant under section 97(1)
- A targeted examination warrant under section 97(2)
- A property interference authorisation under section 5 of the Intelligence Services Act 1994

5.42 Combined warrants may be issued by the Scottish Ministers on the application of the Chief Constable of Police Scotland. This includes a targeted interception warrant, a targeted equipment interference warrant, an authorisation for directed surveillance, an authorisation for intrusive surveillance, and an authorisation under section 93 of the Police Act 1997. Police Scotland are able to conduct intrusive and directed surveillance under RIPSA or RIPA and combinations of warrants can cater for both. It is not, however, possible for a combined warrant to include both an authorisation under RIPA and an authorisation under RIPSA.

5.43 Combined warrants may be issued by the Scottish Ministers on behalf of the Director General of the National Crime Agency, the Commissioners of HMRC, the Chief Constable of the Police Service of Northern Ireland and the Commissioner of the Police of the Metropolis. The combined warrant can include a targeted interception warrant and any combination of a targeted equipment interference warrant and an authorisation under section 93 of the Police Act 1997.

Example 1
An equipment interference agency wishes to conduct equipment interference to acquire private information from a computer and intercept an online video call in the course of its transmission. This activity constitutes both equipment interference and live interception. The interception cannot be authorised as incidental conduct so a combined interception and equipment interference warrant could be obtained. The combined warrant will be issued by the Secretary of State and approved by a Judicial Commissioner. The same rules would apply were the agency to apply for a combined intrusive surveillance and targeted interception warrant.

Example 2
An intelligence agency wish to conduct an operation which involves directed surveillance (provided for under Part 2 of RIPA) and targeted interception. Under Schedule 8 they may wish to combine these applications, so that the combined warrant is issued by the Secretary of State and approved by a Judicial Commissioner. If a law enforcement agency wished to conduct the same activity, they would follow the same process, meaning that the Secretary of State is, as part of the entire application, considering the law enforcement agency's directed surveillance activity as opposed to the internal authorisation that would be required were they to apply individually for a directed surveillance authorisation.

Example 3
An intelligence agency wishes to conduct an operation which involves property interference (provided for under section 5 of the Intelligence Services Act) and targeted interception. Under Schedule 8 they may combine these applications, so that the combined warrant is issued by the Secretary of State. In approving the decision to issue the warrant, the Judicial Commissioner would only consider the application for targeted interception (Note: Property interference under section 5 ISA can also be combined with warrants under Part 2 of RIPA i.e. directed or intrusive surveillance.)

Format of warrant instruments and schedules

Targeted interception warrants

5.44 Each new warrant will typically comprise three sections: a warrant instrument signed by the Secretary of State describing the subject of warrant, a schedule of identifiers listing the communications to be intercepted which each communications service provider will receive as appropriate - and a schedule(s) of subjects. Only the schedule relevant to the communications that can be intercepted by the specified communications service provider should be provided to that communications service provider. Where required, descriptions on the instrument can be in the form of an alias or other description that identifies the subject.

5.45 The warrant instrument will include:

- A statement that it is a targeted interception warrant
- The person to whom it is addressed
- A warrant that relates to a particular person or organisation or to a single set of premises must name or describe that person or organisation or those premises.
- A warrant that relates to a group of persons who share a common purpose or who carry on (or who may carry on) a particular activity must describe that purpose or activity, and name or describe as many of those persons as it is reasonably practicable to name or describe.
- Where the warrant relates to more than one person, organisation or set of premises, and where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation it should describe the operation and names or describe as many of those persons or organisations, or as many of those sets of premises as it is reasonably practicable to name or describe, along with details of how and when the warrant will be updated to comply with section 29(4) or (5).
- A warrant that relates to any testing or training activities must describe those activities and name or describe as many of the persons whose communications will or may be intercepted as it is reasonably practicable to name or describe.
- Where an application is urgent, the supporting justification;
- A warrant reference number.

5.46 The warrant will also comprise two or more schedules - the schedule of subject(s) and schedule(s) of identifiers. The latter will contain:

- The name of the communications service provider, or the other person who is to take action;
- A warrant reference number; and
- A means of identifying the communications to be intercepted or the secondary data to be obtained.[6] The warrant must specify (or describe[7]) the factors or combination of factors that are to be used for identifying the communications. Where the communications are to be identified by reference to a telephone number (for example) the number must be specified by being rendered in its entirety. But where very complex or continually-changing internet selectors are to be used for identifying the communications, those selectors should be described to the degree that is reasonably practicable;

[6] Where a warrant identifies the communications to be intercepted by reference to a number, apparatus or other factors, the warrant authorises the interception or selection of those communications by all correlated numbers, apparatus or factors. For example, where a mobile phone number is specified, that includes not only the phone number given to the user, but also any number or address used to identify that phone or handset to the network or CSP. Such a number or address may be temporary or permanent.

[7] See section 235 of the Act.

Targeted examination warrants

5.47 Each warrant comprises a warrant instrument signed by the Secretary of State listing the subject of the interception selected for examination.

5.48 The warrant instrument will include the details below. Where required, descriptions on the instrument can be.in the form of an alias or other description that identifies the subject.

- A statement that it is a targeted examination warrant;
- The person to whom it is addressed; A means of identifying the communications content that is to be selected for examination. The warrant must specify (or describe[8]) the factors or combination of factors that are to be used for identifying the communications. Where the communications are to be identified by reference to a telephone number (for example) the number must be specified by being rendered in its entirety. But where very complex or continually-changing internet selectors are to be used for identifying the communications, those selectors should be described to the degree that is reasonably practicable;
- A warrant that relates to a particular person or organisation or to a single set of premises must name or describe that person or organisation or those premises.
- A warrant that relates to a group of persons who share a common purpose or who carry on (or who may carry on) a particular activity must describe that purpose or activity, and name or describe as many of those persons as it is reasonably practicable to name or describe.
- Where the warrant relates to more than one person, organisation or set of premises, and where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation it should describe the operation and names or describe as many of those persons or organisations, or as many of those sets of premises as it is reasonably practicable to name or describe.
- A warrant that relates to any testing or training activities must describe those activities and name or describe as many of the persons whose communications content will or may be selected for examination as it is reasonably practicable to name or describe.
- A warrant reference number.

Mutual assistance warrants

5.49 Each mutual assistance warrant will include:

- A statement that it is a mutual assistance warrant;
- The person to who it is addressed;
- 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 that relates to a particular person or organisation or to a single set of premises must name or describe that person or organisation or those premises.
- A warrant that relates to a group of persons who share a common purpose or who carry on (or who may carry on) a particular activity must describe that

[8] See section 235 of the Act.

purpose or activity, and name or describe as many of those persons as it is reasonably practicable to name or describe.
- Where the conduct authorised or required by the warrant is for the purposes of the same investigation or operation it should describe the operation and names or describe as many of those persons or organisations, or as many of those sets of premises as it is reasonably practicable to name or describe.
- A warrant that relates to any testing or training activities must describe those activities and name or describe as many of the persons whose communications will or may be intercepted as it is reasonably practicable to name or describe.
- A warrant reference number

5.50 In addition, where section 38 (special rules for certain mutual assistance warrants) applies, the warrant must contain:

- A statement that the warrant is issued for the purposes of a request for assistance made under an EU mutual assistance instrument or an international mutual assistance agreement (as the case may be) by the competent authorities of a country or territory outside of the United Kingdom and;

- Whichever of the following statements is applicable:

Either:

a) A statement that the interception subject appears to be outside of the United Kingdom, or

b) A statement that the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom.

Authorisation of a targeted warrant

5.51 The Secretary of State may only issue a warrant under section 19 if the Secretary of State considers the following tests are met:

- **The warrant is necessary:**[9]
  a) In the interests of national security;

  b) For the purpose of preventing or detecting serious crime;

  c) In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security. A warrant will only be considered necessary on these grounds if the information relates to the acts or intentions of persons outside the British Islands;

  d) In relation to a mutual assistance warrant for the purpose of giving effect to the provisions of an EU mutual assistance instrument or an international mutual assistance agreement.

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

- **The conduct authorised by the warrant is proportionate to what it seeks to achieve.** In considering necessity and proportionality, the Secretary of State must take into account whether the information sought could reasonably be obtained by other means.

- **There are satisfactory safeguards in place.** The Secretary of State must consider that satisfactory arrangements are in force in relation to the warrant. These safeguards relate to the copying, dissemination, retention of intercepted material and are explained in chapter 9 of this code.

- **The Secretary of State has consulted the Prime Minister** where the additional protection for Members of Parliament and other relevant legislatures applies (see section 94 of the Act).

- **Judicial Commissioner approval.** Except in an urgent case, the Secretary of State may not issue a warrant unless and until the decision to issue the warrant has been approved by a Judicial Commissioner. Section 23 of the Act sets out that the Judicial Commissioner must review the conclusions that have been reached as to whether the warrant is necessary on one or more of the grounds and whether the conduct that would be authorised is proportionate to what is sought to be achieved.

5.52 In reviewing these factors, the Judicial Commissioner must apply judicial review principles. The Judicial Commissioner may speak to the warrant granting department or warrant seeking agency as part of their considerations. If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either:

- not issue the warrant;

- refer the matter to the Investigatory Powers Commissioner for a decision (unless the Investigatory Powers Commissioner has made the original decision).

5.53 If the Investigatory Powers Commissioner refuses the decision to issue a warrant the Secretary of State must not issue the warrant.

5.54 Section 38 of the Act makes clear that there are circumstances where the decision to issue a mutual assistance warrant may be taken by a senior official designated by the Secretary of State for that purpose. This applies if the warrant is for the purposes of giving effect to a request received for assistance made under an EU mutual assistance instrument or an international mutual assistance agreement and either it appears that the interception subject is outside the UK, or the interception to which the warrant relates is to take place in relation only to premises outside the UK.

Power of Scottish Ministers to issue warrants

5.55 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, modification and cancellation arrangements. Sections21 and 22 of the Act make provision for Scottish Ministers to issue targeted interception warrants for serious crime purposes in certain circumstances. Scottish Ministers may issue a targeted interception warrant, a targeted examination warrant or for serious crime purposes providing the warrant, if issued, would relate to a person or group of persons in Scotland or premises which are in Scotland. They may also issue a mutual assistance warrant if it would relate to a person or group of persons, or to premises in Scotland.

5.56 Scottish Ministers may issue a mutual assistance warrant in the circumstances described in section 21(3) and (4):

Per section 21(3):

- That the application requests, in accordance with an EU mutual assistance instrument or international mutual assistance agreement, the provision of assistance in connection with, or in the form of, an interception of communications, or
- That the making of such a request and disclosure in any manner described in the warrant, of any intercepted content or secondary data obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf, and:

  a) The application is made by, or on behalf of, the chief constable of the Police Service of Scotland, or

  b) Is made by, or on behalf of, the Commissioners for HMRC or the Director General of the NCA for the purpose of preventing or detecting serious crime in Scotland.

Per section 21(4):

- That the application is for the issue of a mutual assistance warrant which, if issued, would authorise or require:

  a) The provision or assistance to the competent authorities of a country or territory outside the UK, in accordance with such an instrument or agreement, of any assistance of a kind described in the warrant in connection with or in the form of an interception of communications or

  b) The provision of such assistance and disclosure in any manner described in the warrant of any intercepted content or secondary data obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf and the warrant, if issued, would relate to:

i. A person who is in Scotland, or is reasonably believed by the applicant to be in Scotland, at the time of the issue of the warrant or
ii. Premises which are in Scotland, or are reasonably believed by the applicant to be in Scotland, at that time.

Authorisation of a targeted interception warrant: senior officials and appropriate delegates

5.57 The Act permits that when it is not reasonably practicable for the Secretary of State to sign an interception warrant a delegate may sign the warrant on their behalf. Typically this scenario will arise where the Secretary of State is not physically available to sign the warrant because, for example, they are on a visit or, in the case of a Secretary of State, in their constituency. The Secretary of State must still personally authorise the interception. When seeking authorisation the senior official must explain the case, either in writing or orally, to the Secretary of State and this explanation should include considerations of necessity and proportionality. Once authorisation has been granted the warrant may be signed by a senior official. If the Secretary of State refuses to authorise the warrant, the warrant must not be issued. When a warrant is issued in this way the warrant instrument must contain a statement to that effect. Except in urgent cases the decision to issue the warrant must then be approved by a Judicial Commissioner before the warrant is issued.

Judicial commissioner approval

5.58 Before a targeted warrant can be issued, the Secretary of State's decision to issue it must be approved by a Judicial Commissioner. Section 23 of the Act sets out the test that a Judicial Commissioner must apply when considering whether to approve the decision. This includes reviewing the warrant issuer's conclusion on whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

5.59 In reviewing these factors, the Judicial Commissioner must apply judicial review principles. The Judicial Commissioner may seek clarification from the warrant granting department or warrant seeking agency as part of their considerations.

5.60 If the Judicial Commissioner refuses to approve the decision to issue a warrant the warrant issuer may either:

- not issue the warrant; or,
- refer the matter to the IPC for a decision (unless the IPC has made the original decision).

5.61 If the IPC refuses the decision to issue a warrant the warrant issuer must not issue the warrant. There is no further avenue of appeal available.

5.62 The Act does not mandate how the Judicial Commissioner must show or record their decision. These practical arrangements should be agreed between the relevant public authorities and the Investigatory Powers Commissioner. The Act does not, for example, require the Judicial Commissioner to sign a legal instrument. This means that a Judicial Commissioner can provide oral approval to issue a warrant. It is important that a written record is taken of any such approvals.

Urgent authorisation of a targeted interception warrant

5.63 The Act makes provision for cases in which a targeted interception warrant is required urgently.

5.64 Urgency is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the time available to meet an operational or investigative need. Accordingly, urgent warrants can authorise interception when issued by the issuing authority without prior approval from a Judicial Commissioner. Urgent warrants should fall into at least one of the following three categories:

- Imminent threat to life or serious harm - for example, if an individual has been kidnapped and it is assessed that his life is in imminent danger;
- An intelligence gathering opportunity which is significant because of the nature of the potential intelligence, the operational need for the intelligence is significant, or the opportunity to gain the intelligence is rare or fleeting – for example, a group of terrorists is about to meet to make final preparations to travel overseas;
- A significant investigative opportunity with limited time to act - for example, a consignment of Class A drugs is about to enter the UK and law enforcement agencies want to have coverage of the perpetrators of serious crime in order to effect arrests.

5.65 The decision by the issuing authority to issue an urgent warrant must be reviewed by a Judicial Commissioner within three working days following the day of issue. In the case of warrants signed by a senior official the Judicial Commissioner's review should be on the basis of a written record, including any contemporaneous notes, of any oral briefing (and any questioning or points raised by the Secretary of State) of the Secretary of State by a senior official.

5.66 If the Judicial Commissioner retrospectively agrees to the Secretary of State's issuing of the urgent warrant, and it is still considered necessary and proportionate by the warrant requesting agency, renewal of the urgent warrant may be sought. A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed. If it is renewed it expires after six months, in the same way as non-urgent targeted interception warrants. It is acceptable for the Secretary of State to decide to renew an urgent warrant. In these circumstances, the application to approve the urgent warrant can be presented to the Judicial Commissioner at the same time as they are considering the Secretary of State's decision to renew the warrant.

Warrants ceasing to have effect

5.67 Where a Judicial Commissioner refuses to approve a decision to issue an urgent warrant, the intercepting agency must, as far as reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

5.68 The diagram at Annex A illustrates the authorisation process.

Example A
A suspect is believed to be involved in the illegal sale of military grade weapons and is planning to visit the UK on business. Their travel plans are uncovered at short notice as their passport allows visa-free travel to the UK and they made a late booking. It is a brief visit, only 2 days, beginning in 24hrs time. This will present a unique opportunity to intercept their communications to learn more about their associates here in the UK. An urgent warrant is requested to intercept their communications while in the UK.

Example B
An agent from a hostile nation has been observed trying to build relationships with those with access to critical national infrastructure. There had been little clarity over their intentions, meaning an intrusive interception warrant would not have been proportionate. More information comes to light and it is now suspected that they are trying to buy classified information which could damage national security. They are thought to have had some success in persuading someone to share information and the two are due to communicate imminently. An urgent warrant is requested to intercept their communications and identify the potential seller.

Duration of interception warrants

5.69 A targeted interception warrant, targeted examination warrant or mutual assistance warrant issued using the standard procedure is valid for an initial period of six months. A warrant issued under the urgency procedure is valid for five working days following the date of issue unless renewed by the Secretary of State.

5.70 Upon renewal, warrants are valid for a further period of six months. These dates run from the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed[10]. In practice this means that if a warrant is due to end on 3 March but is renewed on 1 March, the renewal takes effect from 4 March and the renewed warrant will expire on 3 September. An interception warrant may only be renewed in the last 30 days of the period for which it has effect[11].

[10] See section 30 (2)(b)(ii)

[11] See section 35(1)(b)

5.71 Where modifications to an interception warrant are made, the warrant expiry date remains unchanged.

5.72 Where a change in circumstance leads the intercepting agency to consider it no longer necessary, proportionate or practicable for a warrant to be in force, the agency must make a recommendation to the Secretary of State that it should be cancelled with immediate effect.

Modification of targeted warrants

5.73 Warrants issued under Part 2 may be modified under the provisions of section 32 of the Act. Section 32 sets out that both major and minor modifications can be made and the process for authorising such modifications. It is for the warrant requesting agency to initially consider whether the modification being sought is minor or major. All warrants, whether they have been modified or not, will still be subject to oversight by the Investigatory Powers Commissioner. Some circumstances will require both a major and a minor modification to a warrant (for example, where a person is added to a thematic warrant and a factor relating to that person is to be specified). In such a case the authority may apply for the major and minor modifications at the same time, although there is no obligation to do so.

5.74 This section should be read in conjunction with the section in this code on the subject-matter and scope of targeted warrants.

Major Modifications

5.75 A major modification is one in which a name, or description of a person, organisation or set of premises to which the warrant relates is added or varied. For example, adding an associate of a person of intelligence interest to a thematic warrant, in a case where it is reasonably practicable to do so. A major modification of this type cannot be made to a warrant which relates to a 17(1) targeted warrant i.e. where the warrant relates to a particular person, organisation or a single set of premises. A major modification may be made by the following persons in circumstances where the person considers that the modification is necessary on any grounds falling within section 20 of the Act[12]:

- The Secretary of State, in the case of a warrant issued by the Secretary of State
- A member of the Scottish Government, in the case of a warrant issued by the Scottish Ministers, or
- A senior official[13] acting on behalf of the Secretary of State or (as the case may be) the Scottish Ministers.

5.76 As soon as is reasonably practicable after a person makes a major modification of a warrant, a Judicial Commissioner must be notified of the modification and the reason for making it, unless the modification is an urgent modification or sections 26 or 27 apply.

[12] In the case of a warrant issued by the Scottish Ministers the grounds are listed within section 21 of the Act

[13] A senior official in this section is defined at section 33(6))

5.77 In practice, this means that major modifications may be made to targeted thematic warrant to add or vary the name or description of a person, organisation or set of premises to which the warrant relates providing the modification authorises conduct that is within the scope of the original warrant (see section 32(2)(a) and (5)(a)). But where the warrant is not thematic and relates to a particular person, organisation or set of premises), then section 32(3) prohibits modifications to add, vary or remove the name or description of that person, organisation or set of premises. In practice this means that a warrant which relates to a particular person, premises or organisation subject cannot be modified into a thematic warrant; a fresh warrant will be required in these cases. However, there is nothing to prevent the minor modification of both non-thematic and thematic targeted warrants in accordance with section 32(2)(b) by adding a factor identifying additional communications to be intercepted providing those communications fall within the scope of the original warrant.

5.78 Two examples are provided below – the first would not be permitted, but the second would be:

Example of a modification that would NOT be permitted:
An intercepting agency obtains a non-thematic targeted interception warrant relating to a specific serious criminal known as 'Mr. Big'. The Secretary of State, with Judicial Commissioner approval, issues the warrant authorising the interception of Mr. Big's communications. The investigation progresses and the intercepting agency wants to intercept the communications of one of Mr. Big's associates. This would require a new warrant – the warrant against Mr. Big cannot be modified so it is against an additional person.

Example of a modification that would be permitted:
An intercepting agency obtains a targeted thematic interception warrant relating to a specific serious criminal known as 'Mr. Big' and his unidentified associates. The Secretary of State, with Judicial Commissioner approval, issues the warrant authorising the interception of Mr. Big and his unidentified associates investigated under Operation "NAME". The investigation progresses and the intercepting agency wants to intercept of one of Mr. Big's associates. The warrant could be modified to add the associate, and the factors to be used to identify his communications. This would also require a minor

Minor modifications

5.79 A minor modification is the modification of a warrant to remove the name or description of a person, organisation or set of premises, or to add, vary or remove any factor specified in the warrant. For example if a person who is the subject of a non-thematic targeted warrant buys a new mobile phone, adding that second phone number to the warrant would be a minor modification. Minor modifications may also be made to both non-thematic and thematic targeted warrants to add factors identifying additional communications to be intercepted, providing those communications fall within the scope of the original warrant.

Example: A targeted warrant authorises interception of a UK-based company which is believed to be exporting in breach of sanctions. The company acquires new email addresses for its expanding international sales and export function. These email addresses may be added to the warrant by minor modification.

5.80 A minor modification may be made by anyone who can make a major modification, as well as the person to whom the warrant was addressed, or a senior person within the intercepting agency that granted the warrant. Allowing a warrant requesting agency to make minor modifications ensures that the system is operationally agile and the intercepting agency is able to respond quickly when a person changes a phone or the way in which he or she communicates. A minor modification can be made by the following persons:

- The Secretary of State,
- A member of the Scottish Government,
- A senior official[14] acting on behalf of the Secretary of State or member of the Scottish Government, or a person in an intelligence service of equivalent seniority to a member of the Senior Civil Service
- The person to whom the warrant is addressed, or
- A person who holds a senior position in the same intercepting agency as the person to whom the warrant is addressed.

5.81 A minor modification may require a new schedule to be issued to a communications service provider on whom a copy of the warrant has not been previously served. Modifications made in this way will expire at the same time as the warrant expires. There also exists a duty[15] 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.

Administrative clarifications of targeted warrants

5.82 Section 32 (6) makes clear that a major or minor warrant modification is only required where the conduct authorised by the warrant is affected. For example, where more detail is provided for clarification, such as the full name of a person as it becomes known, rather than an alias, the administrative clarification will fall under section 32(6) as long as the subject of interception is still accurately described (i.e. there is no change in the scope of the interception). Nonetheless, thematic warrants should include details of how and when updates to the warrant will be provided.

2. **Example:** A thematic warrant has been issued for interception of a child abuse webforum. The only way that interception can technically be achieved is by using factors to do with the forum space itself: the interception is not effected via factors associated with individual users (for example, name or IP address) which are in any case unknown. If and when the Agency becomes aware of the identity of individual users, the Agency must update the warrant granting department so that as much information is available as possible to the Secretary of State on any persons who are affected by the warrant. However, the conduct authorised by the warrant has not changed.

[14] A senior official in this section is defined at section 33(6).

[15] 34(10)

Urgent major modification of targeted warrants

5.83 Section 33(3) of the Act allows for major modifications to be made to a targeted thematic warrant when it is required as a matter of urgency. A major modification to a thematic warrant, including the adding of new individuals to the warrant, will only be considered urgent if there is a very limited window of opportunity to act. For example, this may include a threat to life situation, where a kidnap has taken place, in the immediate aftermath of a major terrorist incident, or where we have received intelligence that a significant quantity of drugs is about to enter the country.

5.84 In these cases a senior official in the intercepting agency may make the urgent modification but it must be approved by a senior official in the warrant granting department within five working days and the Secretary of State and Judicial Commissioner must be notified as soon as is reasonably practicable. In the event that the warrant granting department do not agree to the urgent modification, the activity conducted under the urgent modification remains lawful but the activity authorised by the modification should cease. The Secretary of State should be informed of the request for an urgent modification whether the modification is agreed to or cancelled by the warrant granting department.

Renewal of targeted interception warrants

5.85 Section 31 of the Act sets out that the Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals of warrants made under Part 2 of the Act should contain an update of the matters outlined in paragraph 5.7. In particular, the applicant should give an assessment of the value of interception to the operation to date and explain why it is considered that interception continues to be necessary for one or more of the grounds in section 20, and why it is considered that interception continues to be proportionate.

5.86 In the case of a targeted examination warrant, the Secretary of State must consider that the warrant continues to be necessary to authorise the selection of intercepted content for examination in breach of the prohibition in section 142(4) of the Act on seeking to identify communications of individuals in the British Islands.

5.87 A relevant mutual assistance warrant may be renewed by a senior official designated by the Secretary of State. In the case of renewal, the instrument renewing the warrant must contain the same detail as set out at paragraph 5.49

5.88 As set out in section 38(5), where a senior official renews a relevant mutual assistance warrant, the instrument renewing the warrant must contain a statement that the renewal is for the purposes of a request for assistance made under an EU mutual assistance instrument or an international mutual assistance agreement by the authorities of a country or territory outside the UK, and either a statement that the interception subject appears to be outside the UK or a statement that the interception to which the warrant related is to take place in relation only to premises outside the UK.

5.89 In all cases, a warrant may only be renewed if the case for renewal has been approved by a Judicial Commissioner.

5.90 A copy of the warrant renewal instrument will be forwarded to all relevant communications service providers on whom a copy of the original warrant have been served, providing they are still actively assisting. A warrant renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Warrant cancellation

5.91 Any of the persons authorised to issue warrants under Part 2 may cancel a warrant at any time. If any of the appropriate persons consider that such a warrant is no longer necessary on grounds falling within section 20 of the Act or that the conduct authorised by the warrant is no longer proportionate, to what is sought to be achieved by that conduct, the person must cancel the warrant. Intercepting agencies will therefore need to keep their warrants under regular review and must notify the Secretary of State if they assess that the interception is no longer necessary or proportionate. In practice, the responsibility to cancel a warrant will normally be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State. The intercepting agency should take steps to cease the interception as quickly as possible if they consider that the warrant is no longer necessary or proportionate – they should not wait until the necessary cancellation instrument has been signed.

5.92 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 the warrant schedule(s) during the preceding twelve months.

6. Bulk interception warrants

6.1 This section applies to the bulk interception of communications by means of a warrant issued under Chapter 1 of Part 6 of the Act. A bulk interception warrant must meet two conditions. The first is that its main purpose must be limited to the interception of overseas-related communications and/or the obtaining of secondary data from such communications. Overseas-related communications are defined at section 128 of the Act as those that are sent or received by individuals outside the British Islands. This condition prevents the issue of a bulk interception warrant with the primary purpose of obtaining communications between people in the British Islands.

6.2 The second condition is that the warrant authorises or requires the person to whom it is addressed to intercept, and/or obtain secondary data from, the communications described in the warrant, as well as to select for examination the intercepted content or secondary data, as specified in the warrant. A bulk interception warrant must set out specified operational purposes (see also "safeguards when selecting for examination intercepted content and secondary data obtained under a bulk warrant" from paragraph 6.50). No intercepted content or secondary data may be selected for examination unless doing so is necessary for one or more of the operational purposes specified on the warrant.

6.3 Bulk interception may be used, for example:

- To establish links between known subjects of interest, improving understanding of their behaviour and the connections they are making or the multiple communications methods they may be using.

- To search for traces of activity by individuals who may not yet be known but who surface in the course of an investigation, or to identify patterns of activity that might indicate a threat to the United Kingdom.

Bulk interception in practice

6.4 Bulk interception warrants authorise a two stage process. First, the interception of communications and/or the obtaining of secondary data from such communications in the course of their transmission and second, the selection for examination of particular communications content or secondary data obtained under the warrant.

Bulk Interception

6.5 A bulk interception warrant will usually be served on a communications service provider to provide assistance with giving effect to it. This will normally provide for the interception of communications from communications links operated by that communications service provider, which run through the physical cables that carry internet traffic. This interception will result in the collection of large volumes of communications and/or data. This is essential to enable communications relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation.

6.6 In contrast to targeted interception warrants, issued under Part 2 of the Act, a bulk interception warrant instrument need not name or describe the interception subject or set of premises in relation to which the interception is to take place. Neither does Chapter 1 of Part 6 impose a limit on the number of communications - which may be intercepted. For example, if the requirements of this chapter are met then the interception of all communications transmitted on a particular route or cable, or carried by a particular communications service provider, could, in principle, be lawfully authorised. This reflects the fact that bulk interception is an intelligence gathering capability, whereas targeted interception is primarily an investigative tool that is used once a particular subject for interception has been identified.

6.7 Due to the global nature of the internet, the route a particular communication will take is hugely unpredictable. This means that a bulk interception warrant may intercept communications between individuals in the British Islands. Section 128(5) of the Act makes clear that a bulk interception warrant authorises the interception of communications that are not overseas-related to the extent this is necessary in order to intercept the overseas-related communications to which the warrant relates.

6.8 When conducting bulk interception, an intercepting agency must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communications links, to identify those individual communications links that are most likely to contain overseas-related communications, which will be relevant to the operational purposes specified on a warrant. This is likely to be a dynamic process due to regular fluctuations in the way data routes across the internet. The intercepting agency must also conduct the interception in ways that limit the collection of communications that are not overseas-related to the minimum level compatible with the objective of intercepting the required overseas-related communications.

6.9 There may be circumstances in which the intercepting agency only considers it necessary to use a bulk interception warrant whose main purpose is to obtain the secondary data from relevant overseas-related communications. Sections 128 and 129 of the Act describe what constitutes secondary data in the context of bulk interception. Secondary data includes systems data that facilitates system or service function and identifying data that may be used to identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service and is also data that describes an event or the location of any person, event or thing.

6.10 The Act therefore enables, at section 128(2), a relevant intercepting agency to obtain a bulk interception warrant whose main purpose is to obtain secondary data from the overseas-related communications described in the warrant. While the main purpose of such a warrant will be limited to the obtaining of secondary data, the warrant will also authorise any conduct it is necessary to undertake to do what is authorised by the warrant. This may include the interception of the content of communications but this is only permitted in so far as it is necessary in order to obtain the secondary data from the communications described in the warrant. In the event that any content is intercepted under a secondary data only warrant, the intercepted content must not be selected for examination.

6.11 Section 128(5)(c) provides that a bulk interception warrant authorises conduct for obtaining related systems data from a communications service provider. This is to enable the intercepting agency to make a request to a relevant communications service provider where that provider may be able to provide additional information about systems data from a communication intercepted in accordance with the warrant, such as in relation to the sender or recipient (or intended sender or recipient) of that communication.

The selection for examination of intercepted content and secondary data obtained under a bulk interception warrant

6.12 Where a bulk interception warrant results in the acquisition of large volumes of communications, the intercepting agency will usually apply a filtering process to discard automatically communications that are unlikely to be of intelligence value. Authorised persons within the intercepting agency may then apply search criteria to select for examination communications content and secondary data that is likely to be of intelligence value in accordance with the operational purposes specified on the warrant.

6.13 Section 134 of the Act requires that a bulk interception warrant must specify the operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination. It is likely that a bulk interception warrant will specify a number of operational purposes as set out at section 134(5).

6.14 When an authorised person within the intercepting agency selects a particular communication for examination, the person must provide an explanation of why it is necessary for one or more of the operational purposes specified on the warrant, and why it is proportionate in the particular circumstances. This process is subject to internal audit and external oversight by the Investigatory Powers Commissioner.

6.15 Where an authorised person wishes to select for examination the content of communications of a person known to be in the British Islands collected under a bulk interception warrant, additional safeguards will apply and a separate application will need to be made for a targeted examination warrant (see also "Safeguards when selecting for examination intercepted content or secondary data obtained under a bulk warrant" and in particular paragraphs 5.9, 6.60 to and 6.61).

Application for a bulk interception warrant

6.16 An application for a bulk interception warrant is made to the Secretary of State. As set out at section 130 of the Act, bulk interception warrants are only available to the intelligence agencies. An application for a bulk interception warrant therefore may only be made by or on behalf of the following persons:

- The Director General of the Security Service.
- The Chief of the Secret Intelligence Service.
- The Director of the Government Communications Headquarters (GCHQ).

6.17 Bulk interception warrants, when issued, are addressed to the person who submitted the application. A copy may then be served on any person who may be able to provide assistance in giving effect to that warrant.

6.18 Prior to submission, each application is subject to a review within the agency making the application. This involves scrutiny by more than one official, who will consider whether the application is necessary for one or more of the permitted statutory purposes (in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security). One of the statutory purposes for which a bulk interception warrant can be issued must always be national security. The scrutiny of the application will also include whether the interception proposed is both necessary and proportionate and whether the examination of intercepted content and secondary data is, or may be, necessary for one or more of the operational purposes specified.

6.19 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 and/or from which secondary data will be obtained, details of any communications service provider(s) and an assessment of the feasibility of the operation where this is relevant to the extent known at the time of the application;[16] and
- Description of the conduct to be authorised, which must be restricted to the interception of overseas-related communications, or the conduct (including the interception of other communications not specifically identified by the warrant as set out at section 128(5)) it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of secondary data.
- The operational purposes for which the content and secondary data may be selected for examination and an explanation of why examination is necessary for those operational purposes proposed in the warrant;
- An explanation of why the interception is considered to be necessary for one or more of the statutory purposes, which must always include an explanation of why the interception is necessary in the interests of national security;
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, explaining why less intrusive alternatives have not been or would not be as effective;
- An assurance that intercepted content and secondary data will be selected for examination only so far as it is necessary for one or more of the operational purposes specified on the warrant and it meets the conditions of section 143 of the Act; and
- An assurance that all content and data intercepted will be kept for no longer than necessary and handled in accordance with the safeguards required by section 141 of the Act.

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

Format of a bulk interception warrant

6.20 Each warrant is addressed to the person who submitted the application. A copy may then be served upon such providers of communications services as he or she believes will be able to assist in implementing the interception. Communications service providers will not receive a copy of the operational purposes specified in the warrant. The warrant should include the following:

- A description of the communications to be intercepted and/or from which secondary data will be obtained;
- The operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination;
- The warrant reference number; and
- Details of the persons who may subsequently modify the operational purposes specified on the warrant in an urgent case.

Additional requirements in respect of warrants affecting overseas operators

6.21 As set out at section 131, additional requirements apply in circumstances where an application for a bulk interception warrant has been made and, were the warrant issued, the Secretary of State considers that a communications service provider outside the United Kingdom is likely to be required to provide assistance in giving effect to it.

6.22 Before deciding to issue the warrant in these circumstances, the Act requires that the Secretary of State must consult the relevant communications service provider. Should the communications service provider have concerns about the reasonableness, technical feasibility or likely cost of providing assistance in giving effect to the warrant, these concerns should be raised during the consultation process.

6.23 Following the conclusion of the consultation process, the Secretary of State will decide whether to issue the warrant. As part of the decision making process, the Secretary of State must take into account, amongst other things, the matters specified in section 131, which are:

- The likely benefits of the warrant;
- The likely number of users (if known) of any telecommunications service which is provided by the operator and to which the warrant relates – this will help the Secretary of State to consider the likely benefits of the warrant.
- The technical feasibility of complying with any requirement that may be imposed on the operator to provide assistance in giving effect to the warrant;
- The likely cost of complying with any such requirement, which will enable the Secretary of State to consider whether the requirement is affordable; and
- Any other effect of the warrant on the operator.

6.24 In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision to issue the warrant, which will include any issues raised by the communications service provider during the consultation.

Authorisation of a bulk interception warrant

Necessity

6.25 Before a bulk interception warrant can be issued, the Secretary of State and Judicial Commissioner must consider that the warrant is necessary for one or more of the statutory purposes, as at 130(1)(b) and (2). One of these statutory purposes must always be national security. If the Secretary of State or Judicial Commissioner is not satisfied that the warrant is necessary in the interests of national security, then it cannot be issued.

6.26 Before a bulk interception warrant can be issued, the Secretary of State and Judicial Commissioner must also consider that the examination of intercepted content or secondary data obtained under the warrant is necessary for one or more of the specified operational purposes (section 130(1)(d)). Setting out the operational purposes on the warrant limits the purposes for which data collected under the warrant can be selected for examination. When considering the specified operational purposes, the Secretary of State and Judicial Commissioner must also be satisfied that examination of the content or data obtained under the warrant for those purposes is necessary for one or more of the statutory purposes set out on the warrant (as at 130(1)(b) and 129(2)). For example, if a bulk interception warrant is issued in the interests of national security and for the purpose of preventing or detecting serious crime, every specified operational purpose on that warrant must be necessary for one or both of these two broader purposes.

6.27 The Secretary of State has a duty to ensure that arrangements are in force for securing that only that content or data which has been considered necessary for examination for a section 130(1)(b) or section 130(2) purpose, and which meets the conditions set out in section 143 is, in fact, selected for examination. The Investigatory Powers Commissioner is under a duty to review the adequacy of those arrangements.

Proportionality

6.28 In addition to the consideration of necessity, the Secretary of State and Judicial Commissioner must be satisfied that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

6.29 In considering whether a bulk interception warrant is necessary and proportionate, the Secretary of State and Judicial Commissioner must take into account whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means (section 2(2)(a) of the Act).

Safeguards

6.30 Before deciding to issue a warrant, the Secretary of State must consider that satisfactory arrangements are in force in relation to the warrant, setting out the safeguards for the copying, dissemination and retention of intercepted content and secondary data. These safeguards are explained in Chapter 9 of this code.

Judicial Commissioner Approval

6.31 Following the decision to issue a bulk interception warrant by the Secretary of State, it must be approved by a Judicial Commissioner.

6.32 Section 132 of the Act sets out the factors that a Judicial Commissioner must consider when deciding whether to approve a bulk interception warrant. The Commissioner must review the Secretary of State's conclusions as to:

- Whether the warrant is necessary and the conduct it authorises is proportionate to what is sought to be achieved; and
- The necessity of examination for each of the specified operational purposes, including whether those operational purposes are necessary for the statutory purposes on the warrant.

6.33 In reviewing these factors, the Judicial Commissioner must apply judicial review principles to a sufficient degree to ensure compliance with the general duties in relation to privacy imposed by section 2 of the Act. The Judicial Commissioner may speak to the warrant granting department or warrant seeking agency as part of their considerations. If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either:

- Not issue the warrant;
- Refer the matter to the Investigatory Powers Commissioner for a decision (unless the Investigatory Powers Commissioner has made the original decision).

6.34 If the Investigatory Powers Commissioner refuses the decision to issue a warrant the Secretary of State must not issue the warrant.

Modification of a bulk interception warrant

6.35 A bulk interception warrant may be modified at any time by an instrument issued by the person permitted to do so by section 137 of the Act. A bulk interception warrant may be modified to add, vary or remove an operational purpose for which intercepted content or secondary data obtained under the warrant may be selected for examination. If the security and intelligence agency requires a change in the scope of the data to be obtained under a warrant or a change to the statutory purpose for which the warrant is issued then an additional or replacement warrant must be sought. Nothing in section 137 of the Act permits, by modification, the addition of an operational purpose which is not relevant to the statutory purposes in relation to which the warrant has been issued.

6.36 In circumstances where a modification is being made to add or vary an operational purpose, the modification must be made by a Secretary of State and must be approved by a Judicial Commissioner before the modification comes into force.

6.37 In circumstances where a bulk interception warrant is being modified to remove an operational purpose, the modification may be made by the Secretary of State or by a senior official acting on their behalf. If a modification, removing an operational purpose, is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it. If at any time the Secretary of State, or a senior official acting on their behalf, considers that a specified operational purpose is no longer necessary in the interests of the statutory purposes listed on the warrant, they shall modify the warrant to remove that operational purpose.

6.38 As set out at paragraphs 6.4-6.15 a bulk interception warrant authorises a two stage process; the interception of communications and/or the obtaining of secondary data, followed by the selection for examination of the content and data collected under the warrant. There will be limited circumstances where it may no longer be necessary, or possible, to continue the first stage of this process, such as where the communications service provider providing assistance with giving effect to the warrant has ceased business. In such circumstances, it may continue to be necessary and proportionate to select for examination the material collected under that warrant. The Act therefore provides that a bulk interception warrant can be modified such that it no longer authorises the interception of communications or the obtaining of secondary data but continues to authorise selection for examination.

6.39 Such a modification may be made by the Secretary of State or by a senior official acting on their behalf. In circumstances where such a modification is being made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

Urgent modifications of a bulk interception warrant

6.40 In urgent cases a modification adding or varying an operational purpose can be made by a Secretary of State or a senior official with the express authorisation of the Secretary of State as set out at section 138 in the Act. An urgent case may be where a sudden terrorist incident requires the urgent selection for examination of the data already held for an operational purpose not listed on the warrant.

6.41 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 date of issue unless it is approved by a Judicial Commissioner. If a Judicial Commissioner refuses to approve the modification, the modification will cease. Any material collected between the modification being made and the Judicial Commissioner reviewing and refusing the modification will be lawful.

Renewal of a bulk interception warrant

6.42 The Secretary of State may renew a warrant within the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect. (section 136 of the Act) with the approval of the Judicial Commissioner. Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 6.19 above. In particular, the applicant must give an assessment of the value of the interception and/or obtaining of secondary data under the warrant to date and explain why it is considered that interception and/or obtaining secondary data continues to be necessary in the interests of national security as well as, where applicable, either or both of the purposes in section 129(2), and why it is considered that the conduct authorised by the warrant continues to be proportionate.

6.43 In deciding to renew a bulk interception warrant, the Secretary of State and Judicial Commissioner must also consider that the examination of intercepted content or secondary data obtained under it continues to be necessary for one or more of the specified operational purposes, and that examination of that content for these purposes is necessary for one or more of the statutory purposes (at 130(1)(b) and 130(2) on the warrant).

6.44 In the case of a renewal of a bulk interception warrant that has been modified so that it no longer authorises or requires the interception of communications or the obtaining of secondary data, it is not necessary for the Secretary of State to consider that interception or the obtaining of secondary data continues to be necessary before making a decision to renew the warrant.

6.45 Where the Secretary of State and Judicial Commissioner are satisfied that the warrant continues to meet the requirements of the Act, the Secretary of State may renew it. The renewed warrant is valid for six months from the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed. In practice this means that if a warrant is due to end on 3 March but is renewed on 1 March, the renewal takes effect from 4 March, and the renewed warrant will expire on 3 September.

6.46 In those circumstances where the assistance of communications service providers has been sought, a copy of the warrant renewal instrument will be forwarded to all those on whom a copy of the original warrant instrument has been served, providing they are still actively assisting. A renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Warrant cancellation

6.47 The Secretary of State, or a senior official acting on their behalf, may cancel a bulk interception warrant at any time. Such persons must cancel an interception warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on the grounds of any one of the statutory purposes (at 130(1)(b) or 130(2)) for which it was issued. Such persons must also cancel a warrant if, at any time before its expiry date, he or she is satisfied that the examination of communications content and/or secondary data is no longer necessary for any of the operational purposes specified on the warrant. Intercepting agencies will therefore need to keep their warrants under regular review and must notify the Secretary of State if they assess that the interception is no longer necessary. In practice, the responsibility to cancel a warrant will normally be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State. The intercepting agency should take steps to cease the interception as quickly as possible if they consider that the warrant is no longer necessary or proportionate – they should not wait until the necessary cancellation instrument has been signed.

6.48 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.

6.49 The cancellation of a warrant does not prevent the Secretary of State, with Judicial Commissioner approval, issuing a new warrant, covering the same, or different communications and operational purposes, in relation to the same communications service provider in the future should it be considered necessary and proportionate to do so. Where there is a requirement to modify the warrant, other than to vary the operational purposes for which the data can be selected for examination, then the warrant may be cancelled and a new warrant issued in its place.

Safeguards when selecting for examination intercepted content or secondary data obtained under a bulk warrant

6.50 Section 143 of the Act provides specific safeguards relating to the selection for examination of intercepted content and secondary data acquired through a bulk interception warrant. References to examination of intercepted content or secondary data are references to it being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.

6.51 Sections 143(1) and (2) make clear that selection for examination may only take place for one or more of the operational purposes that are specified on the warrant, in line with section 133 of the Act. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination, rather than limiting the information which can be examined per se, and no official is permitted to gain access to the data other than as permitted by these purposes. Intercepted content and secondary data selected for examination for an operational purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained on any relevant ground.

6.52 The security and intelligence agencies need to retain the operational agility to respond to developing and changing threats and the range of operational purposes that may need to be specified on a bulk warrant needs to reflect this. New operational purposes will be required over time. Section 134 of the Act makes clear that the heads of the security and intelligence agencies must maintain a central list of all of the operational purposes, separate to individual bulk warrants, which they consider are purposes for which intercepted content or secondary data may be selected for examination. The maintenance of this list will ensure the agencies are able to assess and review all of the operational purposes that are, or could be, specified across the full range of their bulk warrants at a particular time to ensure these purposes remain up to date, relevant to the current threat picture and, where applicable, the intelligence priorities set by the National Security Council. The central list of operational purposes will not be limited to operational purposes relevant to bulk interception warrants. This list must provide a record of all of the operational purposes that are specified, or could be specified, on any bulk interception, bulk acquisition, bulk equipment interference or bulk personal dataset warrant and, as far as possible, the operational purposes specified on the list should be consistent across these capabilities. Some operational purposes on the central list will be consistent across the three agencies, although some purposes will be relevant to a particular agency or two of the three, reflecting differences in their statutory functions.

6.53 Section 134 also makes clear that an operational purpose may not be specified on an individual bulk warrant unless it is a purpose that is specified on the central list maintained by the heads of the security and intelligence agencies. And before an operational purpose may be added to that list, it must be approved by the Secretary of State. In practice, the addition of one operational purpose to the list will often require the approval of more than one Secretary of State. For example, where an operational purpose is being added to the list that is likely to be specified on bulk warrants issued to each of the three security and intelligence agencies, that operational purpose will need to be approved by both the Home Secretary and Foreign Secretary

6.54 Section 130 makes clear that the operational purposes specified on a bulk warrant must relate to one or more of the statutory purposes specified on that warrant. However, section 134 makes clear that it is not sufficient for any operational purpose simply to use the wording of one of the statutory purposes. The Secretary of State may not approve the addition of an operational purpose to the central list – and therefore to any bulk warrants – unless he or she is satisfied that the operational purpose is specified in a greater level of detail than the relevant statutory purposes. Operational purposes must therefore describe a clear requirement and contain sufficient detail to satisfy the Secretary of State that intercepted content or secondary data may only be selected for examination for specific reasons.

6.55 Section 137 of the Act provides for a bulk interception warrant to be modified such that the operational purposes specified on it can be added to or varied. Such a modification is categorised as a major modification and therefore must be made by the Secretary of State and approved by a Judicial Commissioner before the modification may take effect. In such circumstances, and as outlined above, the provisions at section 134 also require that the operational purpose must be approved by the Secretary of State for addition to the central list. If the Secretary of State does not approve the addition of the purpose to the list, the modification to the warrant (to add a new operational purpose) may not be made. The Bill therefore creates a strict approval process in circumstances where an intelligence agency identifies a new operational purpose, which they consider needs to be added to a bulk warrant. The Secretary of State must agree that the operational purpose is a purpose for which selection for examination may take place, and that it is described in sufficient detail such that it should be added to the central list. In addition, the Secretary of State must also consider that the addition of that purpose to the relevant bulk warrant is necessary, taking into account the particular circumstances of the case, before making the modification, and the decision to add the operational purpose must also be approved by a Judicial Commissioner.

6.56 In addition to the central list of operational purposes having to be approved by the Secretary of State, section 134 makes clear that it must also be reviewed on an annual basis by the Prime Minister and it must be shared every three months with the Intelligence and Security Committee.

6.57 Although bulk interception warrants are authorised for the purpose of acquiring overseas-related communications, section 128(5) of the Act makes clear that a bulk interception warrant can authorise the interception of communications that are not overseas-related to the extent this is necessary in order to intercept the overseas-related communications to which the warrant relates. Operational purposes specified on the central list maintained by the heads of the security and intelligence agencies –and on individual bulk interception warrants – may therefore include purposes that enable the selection for examination of intercepted content or secondary data of individuals in the UK. The safeguards in section 143 of the Act ensure that where the content of communications are selected for examination by any criteria referable to an individual known to be in the British Islands at that time, a targeted examination warrant must be obtained under Part 2 of the Act authorising the selection for examination of that content (see also Chapter 5)[17].

6.58 More than one operational purpose may be specified on a single bulk warrant; this may, where the necessity and proportionality test is satisfied, include all operational purposes currently specified on the central list maintained by the heads of the security and intelligence agencies. In the majority of cases, it will be necessary for bulk interception warrants to specify the full range of operational purposes in relation to the selection for examination of intercepted content. This reflects the fact that bulk interception is a strategic capability and overseas-related communications relevant to multiple operational purposes will necessarily be transmitted and intercepted together under the authority of a bulk interception warrant.

[17] Where there is a change of circumstances such that a person whose communications' content is being selected for examination enters, or is discovered to be in the British Islands, sections 134(5) and (6) provide for a continuity arrangement. See paragraph 6.65 of this code

6.59 Other than in exceptional circumstances, it will always be necessary for every warrant application to require the full range of operational purposes to be specified in relation to the selection for examination of secondary data obtained under bulk interception warrants.

6.60 As well as being necessary for one of the operational purposes, any selection for examination of intercepted content or secondary data must be necessary and proportionate.

6.61 In general, automated systems must, where technically possible, be used to effect the selection in accordance with section 143 of the Act. As an exception, intercepted content and secondary data may be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the content and/or secondary data falls within the main categories to be selected under the specified operational purposes, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary on the grounds specified in sections 130(1)(b) and 130(2) of the Act. Once those functions have been fulfilled, any copies made of the content or data for those purposes must be destroyed in accordance with section 141(5) of the Act. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the Investigatory Powers Commissioner during his or her inspections.

6.62 Content and data collected under a bulk interception warrant should be selected for examination only by authorised persons who receive regular mandatory training regarding the provisions of the Act and specifically the operation of section 143 and the requirements of necessity and proportionality. These requirements and procedures must be set out in internal guidance provided to all authorised persons and the attention of all authorised persons must be specifically directed to the statutory safeguards. All authorised persons must be appropriately vetted.

6.63 Prior to an authorised person being able to select for examination, a record[18] should be created setting out why access to the content or data is necessary in pursuance of section 143 and the applicable operational purpose(s), and why such access is proportionate. Save where the content/data or automated systems are being checked as described in paragraph 6.63, the record must indicate, by reference to specific factors, the content or data to which access is being sought and systems should, to the extent possible, prevent access to it unless such a record has been created. Where it is anticipated that the selection for examination is likely to give rise to collateral intrusion into privacy, the reasons this is considered proportionate, and any steps to minimise it, must also be recorded. All records must be retained in accordance with agreed policy for the purposes of subsequent examination or audit.

6.64 Access to the content as described in paragraph 6.63 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 the 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.

[18] Any such record should be made available to the Commissioner on request for purposes of oversight.

6.65 Periodic audits should be carried out to ensure that the requirements set out in section 143 of the Act are being met. These audits must include checks to ensure that the records requesting selection for examination have been correctly compiled, and specifically, that the content or data requested falls within operational purposes the Secretary of State has considered necessary for examination. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards must be reported to the Investigatory Powers Commissioner. Where appropriate, all intelligence reports generated by the authorised persons must be subject to a quality control audit.

6.66 The Secretary of State must ensure that the safeguards are in force before any interception under a bulk interception warrant can begin. The Investigatory Powers Commissioner is under a duty to review the adequacy of the safeguards.

Selection for examination of intercepted content in breach of the section 143(4) prohibition

6.67 Any selection for examination of the content of the communications intercepted must also meet the selection conditions set out at section 143(3). Section 143(4) prohibits the selection for examination of intercepted content using criteria referable to an individual known to be in the British Islands. Selection in breach of this prohibition is only permitted where:

- A targeted examination warrant has been issued under Part 2 authorising the selection for examination of the intercepted content; or
- The selection for examination in breach of the prohibition is authorised by section 143(5).

6.68 Selection for examination in breach of the prohibition in section 143(4) of the Act may be authorised by section 143(5). Section 143(5) addresses cases where there is a change of circumstances such that a person whose content is being selected for examination enters or is discovered to be in the British Islands, for example where a member of an international terrorist or organised crime group travels into the UK. To enable the selection for examination to continue, sections 143(5) and 143(6) of the Act provide for a senior official to give a written authorisation for the continued selection for examination of intercepted content relating to that person for a period of five working days. Any selection for examination after that point will require the issue of a targeted examination warrant, issued by the Secretary of State and approved by a Judicial Commissioner. Where selection for examination is undertaken in accordance with section 143(5) the Secretary of State must be notified.

7. Implementation of warrants and communications service provider compliance

7.1 After a warrant has been issued, it will be forwarded to the person to whom it is addressed – i.e. the intercepting agency which submitted the application.

7.2 Section 39 of the Act then allows the intercepting agency to carry out the interception, and to require the assistance of other persons in giving effect to the warrant. Section 39 makes clear that the warrant may be served on any person, inside or outside the UK, who is required to provide assistance in relation to that warrant. The same process applies for bulk interception warrants and is set out at section 140 of the Act.

7.3 Where a copy of an interception warrant has been served on anyone providing a postal service or a telecommunications service, or who has control of a telecommunications system in the UK, that person is under a duty to take all such steps for giving effect to the warrant as are notified to him or her by or on behalf of the person to whom the warrant is addressed. This applies to any company offering services to customers in the UK, irrespective of where the company is based. Section 41 sets out the means by which that duty may be enforced.

7.4 Section 40 of the Act provides that service of a copy of a targeted interception warrant on a person outside the UK may (in addition to electronic or other means of service) be effected in any of the following ways (section 139 of the Act makes clear that sections 41 and 40 apply in relation to a bulk interception warrant as they do for a targeted interception warrant):

- By serving it at the person's principal office within the UK or, if the person does not have an office in the UK, at any place in the UK where the person carries on business or conducts activities;
- At an address in the UK specified by the person;
- By making it available for inspection at a place in the UK (if neither of the above two methods are reasonably practicable). The intercepting agency must take steps to bring the contents of the warrant to the attention of the relevant person.

Provision of reasonable assistance to give effect to a warrant

7.5 Any communications service provider may be required to provide assistance in giving effect to an interception warrant. A warrant can only be served on a person who is capable of providing the assistance required by the warrant. The Act places a requirement on communications service providers to take all such steps for giving effect to the warrant as are notified to them (section 41 and section 139). The duty to comply with the warrant can only be enforced against a person who is capable of complying with it. Knowingly failing to comply is an offence which, on summary conviction in the UK, may result in imprisonment and/or a fine. Where a technical capability notice is in place, a communications service provider will be considered as having put in place the capabilities specified in that notice when consideration is given to their compliance with the obligation.

7.6 The steps which may be required by communications service providers are limited to those which it is reasonably practicable to take (section 41(4)). When considering this test, section 41(5)(a) specifies that regard must be given to any requirements or restrictions under the law of the country where the communications service provider is based that are relevant to the taking of those steps. It also makes clear the expectation that communications service providers will seek to find ways to comply in a way that avoids such conflicts of law.

7.7 Such a conflict of law will be avoided when complying with a warrant under the auspices of a relevant international agreement between the UK and the jurisdiction in which the communications service provider's primary office is based. Where the warrant served is of a kind that is included within the scope of the relevant international agreement, there is no legal limitation on the communications service provider's ability to comply with the warrant. For the avoidance of doubt, where a communications service provider gives effect to a warrant which falls within the scope of any relevant international agreement, the company will have complied with the obligation imposed by the warrant and enforcement action cannot be taken.

7.8 What is reasonably practicable will be considered on a case-by-case basis, taking into account the individual circumstances of the relevant communications service provider.

7.9 Section 130 details the additional requirements in respect of circumstances where an application for a bulk interception warrant has been made and the Secretary of State considers that a communications service provider outside the UK is likely to be required to provide assistance in giving effect to the warrant if it is issued. This section makes clear that the Secretary of State must consult the communications service provider before issuing the warrant and that they must take into account the likely benefits of the warrant, the likely number of users (if known) of the service provided by the communications service provider to which the warrant relates, the technical feasibility, cost and any other effect of the warrant on the communications service provider.

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

- A copy of the signed and dated warrant instrument; and/or

- A copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant. Targeted interception and mutual assistance warrants must describe the communications to be intercepted by specifying the addresses, numbers, apparatus, or other factors, or combination of factors that are to be used for identifying the communications to be intercepted but any part of this may be excluded from the parts of the warrant provided to a specific communications service provider. Bulk interception warrants must specify the operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination but communications service providers will not receive a copy of the operational purposes specified in the warrant.
- An optional covering document from the intercepting agency (or the person acting on behalf of the agency) may also be provided 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 communications service providers who maintain an interception capability. The communications service provider should be provided with enough information to enable them to carry out the interception in relation to their system(s) and will not necessarily be provided with all the information contained in the warrant.

7.11 Clause 215 provides that disclosures can be made to the Investigatory Powers Commissioner. This includes disclosures made by communications service providers who can contact the Commissioner at any time to request advice and guidance.

Duty not to disclose the existence of a warrant

7.12 For guidance on the provision for communications service providers to be able to publish information in relation to the number of warrants they have given effect to, see paragraph 9.3.

Contribution to costs for giving effect to an interception warrant

7.13 Section 222 of the Act recognises that communications service providers incur expenses in complying with requirements in the Act, including the interception of communications in response to requests under Part 2 of the Act. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.

7.14 Public funding and support is made available to communications service providers to ensure that they can provide, outside of their normal business practices, an effective and efficient response to public authorities' necessary, proportionate and lawful requirements for the interception of communications in support of their investigations and operations to protect the public and to bring to justice those who commit crime.

7.15 It is legitimate for a communications service provider to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to facilitate the timely implementation of an interception warrant. This is especially relevant for communications service providers which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke systems. However, this category of costs will not in most cases include specific staff benefits or arrangements made in line with the terms and conditions of employment, such as pension payments. Such matters are arranged between the employer and employee and the Government does not accept liability for such costs.

7.16 Contributions may also be appropriate towards costs incurred by a communications service provider which needs to update its systems to maintain, or make more efficient, its interception processes. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the interception of communications.

7.17 Any communications service provider seeking to recover appropriate contributions towards its costs should make available to the Government such information as the Government requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the communications service provider.

7.18 Any communications service provider that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made. This is to ensure that expenditure has been incurred for the stated purpose. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

8. Maintenance of a technical capability

8.1 Communications service providers may be required under section 229 of the Act to provide a technical capability to give effect to interception, equipment interference, bulk acquisition warrants or communications data acquisition authorisations. The purpose of maintaining a technical capability is to ensure that, when a warrant or authorisation is served, companies can give effect to it securely and quickly. Small companies (with under 10,000 users) will not be obligated to provide a permanent interception or equipment interference capability, although they may be obligated to give effect to a warrant.

8.2 The Secretary of State may give a relevant communications service provider a "technical capability notice" imposing on the relevant operator obligations specified in the notice, and requiring the person to take all steps specified in the notice. In practice, notices will only be given to communications service providers that are likely to be required to give effect to warrants or authorisations on a recurrent basis.

8.3 The obligations the Secretary of State considers reasonable to impose on communications service providers are set out in regulations made by the Secretary of State and approved by Parliament, and may include (amongst others) obligations of the sort set out at section 229(5) of the Act:

- Obligations to provide facilities or services of a specified description;
- Obligations relating to apparatus owned or operated by a relevant operator;
- Obligations relating to the removal of electronic protection applied by or on behalf of the relevant operator on whom the obligation has been placed to any communications or data;
- Obligations relating to the security of any postal or telecommunications services provided by the relevant operator;
- Obligations relating to the handling or disclosure of any content or data.

8.4 An obligation placed on a communications service provider to remove encryption only relates to electronic protections that the company has itself applied to the intercepted communications (and secondary data), or where those protections have been placed on behalf of that communications service provider, and not to encryption applied by any other party. The purpose of this obligation is to ensure that the content of communications can be provided to the intercepting agencies in intelligible form. References to protections applied on behalf of the communications service provider include circumstances where the communications service provider has contracted a third party to apply electronic protections to a telecommunications service offered by that communications service provider to its customers.

8.5 In the event that a number of communications service providers are involved in the provision of a service, the obligation to provide a capability, and to remove encryption, will be placed on the communications service provider which has the technical capability to give effect to the notice and on whom it is reasonably practicable to impose these requirements. It is possible that more than one communications service provider will be involved in the provision of the interception capability, particularly if more than one communications service provider applies electronic protections to the relevant communications and secondary data.

8.6 While an obligation to remove encryption may only relate to protections applied by or on behalf of the company on whom the obligation is placed, there will also be circumstances where a communications service provider removes encryption from communications for their own business reasons. Where this is the case, an intercepting agency will also require the communications service provider, where applicable and when served with a warrant, to provide those communications in an intelligible form.

Consultation with service providers

8.7 Before giving a notice, the Secretary of State must consult the communications service provider[19]. In practice, informal consultation is likely to take place long before a notice is given. The Government will engage with communications service providers who are likely to be subject to a notice in order to provide advice and guidance, and prepare them for the possibility of receiving a notice.

8.8 In the event that the giving of a notice to a communications service provider is deemed appropriate, the Government will take steps to consult the communications service provider formally before the notice is given. Should the communications service provider have concerns about the reasonableness, cost or technical feasibility of requirements to be set out in the notice, these should be raised during the consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process.

Matters to be considered by the Secretary of State

8.9 Following the conclusion of consultation with a communications service provider, the Secretary of State will decide whether to give a notice. This consideration should include all the aspects of the proposed notice. It is an essential means of ensuring that the notice is necessary and proportionate to what is sought to be achieved, and that proper processes have been followed.

8.10 As part of the decision, the Secretary of State must take into account, amongst other factors, the matters specified in section 231(3):

- The likely benefits of the notice – this may take into account projected as well as existing benefits.
- The likely number of users (if known) of any postal or telecommunications service to which the notice relates – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the technical capability notice.
- The technical feasibility of complying with the notice – taking into account any representations made by the communications service provider and giving specific consideration to any obligations in the notice to remove electronic protections (as described at 231(4)).

[19] See section 231(2).

- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the communications service provider as part of the notice, such as those relating to security. This should also include specific consideration to the likely cost of complying with any obligations in the notice to remove electronic protections. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money.

- Any other effect of the notice on the communications service provider – again taking into account any representations made by the company.

8.11 In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision. Clause 2 of the Act also requires the Secretary of State to give regard to the following when giving, varying or revoking a notice:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means,

- the public interest in the integrity and security of telecommunication systems and postal services, and

- any other aspects of the public interest in the protection of privacy.

8.12 The Secretary of State may give a notice after considering of the points above if he or she considers that the notice is necessary, and that the conduct required is proportionate to what is sought to be achieved. The obligations set out in the notice must be reasonable, and the Secretary of State must ensure that communications service providers are capable of providing the necessary technical assistance.

8.13 Before the notice may be given, a Judicial Commissioner must approve the Secretary of State's decision to give a notice. In deciding whether to approve the Secretary of State's decision to give a relevant notice, a Judicial Commissioner must review the Secretary of State's conclusions regarding the necessity of the notice and the proportionality of the conduct required by the notice.

Giving a notice

8.14 Once the Secretary of State has made a decision to give a notice and it has been approved by a Judicial Commissioner, arrangements will be made for this to be given to the communications service provider. During consultation, it will be agreed who within the company should receive the notice and how it should be provided (i.e. electronically or in hard copy). If no recipient is agreed, then the notice will be issued to a senior executive within the company.

8.15 Section 231(6) provides that technical capability notices may be given to, and, obligations imposed on communications service providers located outside the UK and may require things to be done outside the UK. Where a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given to the communications service provider[20]:

- By delivering it to the person's principal office within the UK or, if the person does not have an office in the UK, to any place in the UK where the person carries on business or conducts activities;

- At an address in the UK specified by the person.

8.16 The person or company to whom a notice is given will be provided with a handbook which will contain the basic information they will require to respond to requests for reasonable assistance in relation to the interception of communications.

8.17 As set out in section 229(7), the notice will specify the period within which the communications service provider must undertake the steps specified in the notice. It will often be the case that a notice will require the creation of dedicated systems. The time taken to design and construct such a system will be taken into account and, accordingly, different elements of the notice may take effect at different times.

8.18 A person to whom a technical capability notice is given is under a duty to comply with the notice. In respect of a technical capability notice to give effect to equipment interference or bulk acquisition warrants, the duty to comply with a technical capability notice is enforceable against a person in the UK by civil proceedings by the Secretary of State[21]. The duty to comply with a technical capability notice to give effect to interception warrants and CD authorisations is enforceable against a person in the UK and a person outside the UK by civil proceedings by the Secretary of State[22].

[20] See section 231 (6).

[21] See section 231(10)(a)

[22] See section 231(10)(b)

Disclosure of technical capability notices

8.19 The Government does not publish or release identities of those subject to a technical capability notice, as to do so may identify operational capabilities or harm the commercial interests of companies acting under a notice. Should criminals become aware of the capabilities of law enforcement, they may alter their behaviours and change communications service provider, making it more difficult to detect their activities of concern.

8.20 Any person to whom a technical capability notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence or contents of that notice to any person[23].

8.21 Section 231(8) of the Act provides for the person to disclose the existence and contents of a technical capability notice with the permission of the Secretary of State. Such circumstances are likely to include disclosure:

- To a person (such as a system provider) who is working with the communications service provider to give effect to the notice;
- To relevant oversight bodies;
- To regulators in exceptional circumstances where information relating to a capability may be relevant to their enquiries;
- To other communications service providers subject to a technical capability notice to facilitate consistent implementation of the obligations; and
- In other circumstances notified to and approved in advance by the Secretary of State.

Regular review

8.22 The Secretary of State must keep technical capability notices under review. This helps to ensure that the notice itself, or any of the requirements specified in the notice, remain necessary and proportionate.

8.23 It is recognised that, after a notice is given, the communications service provider will require time to take the steps outlined in the notice and develop the necessary capabilities. Until these capabilities are fully operational, it will be difficult to assess the benefits of a notice. As such, the first review should not take place until after these are in place.

8.24 A review of a technical capability notice will take place at least once every two years once capabilities are in place. However, the exact timing of the review is at the Secretary of State's discretion.

8.25 A review may be initiated earlier than scheduled for a number of reasons. These include:

[23] See section 231(8)

- a significant change in demands by the intercepting agencies that calls into question the necessity and proportionality of the notice as a whole, or any element of the notice;

- a significant change in the communications service provider's activities or services; or

- a significant refresh or update of communications service provider's systems.

8.26 The process for reviewing a notice requires the Government to consult the communications service provider and for the Secretary of State to determine whether the notice remains necessary and proportionate.

8.27 A review may recommend the continuation, variation or revocation of a notice. The relevant communications service provider and the operational agencies will be notified of the outcome of the review.

Variation of technical capability notices

8.28 The communications market is constantly evolving and communications service providers subject to technical capability notices will often launch new services.

8.29 Communications service providers subject to a technical capability notice must notify the Government of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require the communications service provider company to provide a technical capability on the new service.

8.30 Small changes, such as upgrades of systems which are already covered by the existing notice, can be agreed between the Government and communications service provider in question. However, significant changes will require a variation of the technical capability notice.

8.31 Section 232 of the Act provides that technical capability notices can be varied by the Secretary of State. There are a number of reasons why a notice might be varied. These include:

- a communications service provider launching new services;
- changing law enforcement demands and priorities;
- a recommendation following a review (see section above); or
- to amend or enhance the security requirements.

8.32 Where a communications service provider has changed name, for example as part of a rebranding exercise or due to a change of ownership, the Government, in consultation with the communications service provider, will need to consider whether the existing notice should be varied.

8.33 Before varying a notice, the Government will consult the intercepting agencies to understand the operational impact of any change to the notice, and the communications service providers to understand the impact on them, including any technical implications. Once this consultation process is complete, the Secretary of State will consider whether it is necessary to vary the notice and whether the new requirements imposed by the notice as varied are proportionate to what is sought to be achieved by that conduct.

8.34 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraphs 8.7 - 8.13.

8.35 Once a variation has been agreed by the Secretary of State, arrangements will be made for the communications service provider to receive notification of this variation and details of the timeframe in which the variation needs to be enacted by the communications service provider. The time taken to implement these changes will be taken into account and, accordingly, different elements of the variation may take effect at different times.

Revocation of technical capability notices

8.36 A technical capability notice must be revoked (in whole or in part) if it is no longer necessary to require a communications service provider to provide a technical capability.

8.37 Circumstances where it may be appropriate to revoke a notice include where a communications service provider no longer operates or provides the services to which the notice relates, where operational requirements have changed, or where such requirements would no longer be necessary or proportionate.

8.38 The revocation of a technical capability notice does not prevent the Secretary of State issuing a new technical capability notice, covering the same, or different, services to the same communications service provider in the future should it be considered necessary and proportionate to do so.

Referral of technical capability notices

8.39 The Act includes clear provisions for communications service providers to request a review of the requirements placed on them in a technical capability notice should they consider these to be unreasonable. A person may refer the whole or any part of a technical capability notice back to the Secretary of State for review under section 233 of the Act.

8.40 The circumstances and timeframe within which a communications service provider may request a review are set out in regulations made by the Secretary of State and approved by Parliament. These circumstances include opportunities for a communications service provider to refer a notice for review following the receipt of a new notice or the notification of a variation to a notice. Details of how to submit a notice to the Secretary of State for review will be provided either before or at the time the notice is served.

8.41 Before deciding the review, the Secretary of State must consult and take account of the views of the Technical Advisory Board (TAB) and a Judicial Commissioner. The Board must consider the technical requirements and the financial consequences of the notice for the person who has made the referral. The Commissioner will consider whether the notice is proportionate.

8.42 The Commissioner and the TAB must give the relevant communications service provider and the Secretary of State the opportunity to provide evidence and make representations to them before reaching their conclusions. Both bodies must report these conclusions to the person who made the referral and the Secretary of State.

8.43 After considering reports from the TAB and the Commissioner, the Secretary of State may decide to vary, revoke or confirm the effect of the notice. Where the Secretary of State decides to confirm or vary the notice, the Investigatory Powers Commissioner must approve the decision. Until the Secretary of State's decision is approved, there is no requirement for the communications service provider to comply with the notice so far as referred. The communications service provider will remain under obligation to provide assistance in giving effect to an interception warrant, as set out in section 41 of the Act.

Contribution of costs for the maintenance of a technical capability

8.44 Section 225 of the Act recognises that communications service providers incur expenses in complying with requirements in the Act, including notices to maintain permanent interception capabilities under Part 9. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.

8.45 Communications service providers that are subject to a technical capability notice under Part 9 of the Act are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a technical capability notice and the Act.

8.46 Any contribution towards these costs must be agreed by the Government before work is commenced by a communications service provider and will be subject to the Government considering, and agreeing, the technical capability proposed by the communications service provider.

8.47 Costs that may be recovered could include those related to the procurement or design of systems required to intercept communications, their testing, implementation, continued operation and, where appropriate, sanitisation and decommissioning. Certain overheads may be covered if they relate directly to costs incurred by communications service providers in complying with their obligations outlined above. This is particularly relevant for communications service providers that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems. However, this category of costs will not in most cases include specific staff benefits or arrangements made in line with the terms and conditions of employment, such as pension payments. Such matters are arranged between the employer and employee and the Government does not accept liability for such costs.

8.48 It may also be appropriate for the Government to contribute towards costs incurred by a communications service provider to update its systems to maintain, or make more efficient, its interception process. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the use of such services. However, where a communications service provider expands or changes its network for commercial reasons, it is expected to meet any capital costs that arise.

General considerations on appropriate contributions

8.49 Any communications service provider seeking to recover appropriate contributions towards its costs should make available to the Government such information as the Government requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the communications service provider.

8.50 As costs are reimbursed from public funds, communications service providers should take into account value for money when procuring, operating and maintaining the infrastructure required to comply with a notice. As changes to business systems may necessitate changes to interception systems, communications service providers should take this into account when altering business systems and must notify the Government of proposed changes.

8.51 Any communications service provider that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made. This is to ensure that expenditure has been incurred for the stated purpose. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

Power to develop compliance systems

8.52 In certain circumstances it may be more economical for products to be developed centrally, rather than communications service providers or public authorities creating multiple different systems to achieve the same end. Where multiple different systems exist, it can lead to increased complexity, delays and higher costs when updating systems (for example, security updates).

8.53 Section 226 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop consistent systems for use by communications service providers to intercept communications and secondary data. Such systems could operate in respect of multiple powers under the Act.

8.54 Where such systems are developed for use by communications service providers, the Government will work closely with communications service providers to ensure the systems can be properly integrated into their networks.

Security, integrity and disposal of interception capabilities

8.55 The obligations the Secretary of State considers reasonable to impose on communications service providers in technical capability notices may include (amongst others) obligations relating to the security of any postal or telecommunications services provided by the relevant operator.

8.56 Communications service providers must maintain physical, document, operational and non-operational information technology, and personnel security to standards as specified in the Cabinet Office Security Policy Framework, subject to guidance from the National Technical Assistance Centre (NTAC). Communications service providers must also implement the Government's Information Assurance Maturity Model in conjunction with CESG/CCP[24] approved consultant to identify their level of information security. The results of this assessment should be shared with NTAC.

8.57 Specific security requirements relate to a number of broad areas – the security and integrity of interception identifiers/factors and delivery of intercept product, and the destruction of interception identifiers/factors.

8.58 Detail on the security arrangements to be put in place by communications service providers may be included in the technical capability notices given to a communications service provider, in accordance with section 229(5) of the Act. A Service Level Agreement will also be negotiated between the Government and the communications service provider. This document will provide detail of how the obligations imposed by a technical capability notice will be effected, including those that relate to security.

8.59 The scope of the security controls defined within this section apply to all dedicated IT systems that are used to access, support or manage dedicated interception systems. It also applies to all communications service provider (or third party) operational and support staff who have access to such systems.

8.60 Systems holding intercept material will be securely separated by technical security measures (e.g. a firewall) from a communications service provider's business systems. However, interception solutions may make use of equipment currently in place at the communications service provider's facilities.

8.61 Where interception identifiers/factors are retained in business or shared systems, or where business systems are used to access, support or manage interception systems, these will be subject to specific security controls and safeguards as agreed with the Government.

Security

8.62 The security put in place at a communications service provider's facilities will comprise four key areas:

- Physical security e.g. buildings, server cages, CCTV;
- Technical security e.g. firewalls and anti-virus software;
- Personnel security e.g. staff security clearances and training; and

[24] For further details, please see guidance on CESG website: www.cesg.gov.uk.

- Procedural security e.g. processes and controls.

8.63 As each of these broad areas is complementary, the balance between these may vary e.g. a communications service provider with slightly lower personnel security will require stricter technical and procedural controls. The specific security arrangements in place will be agreed in confidence between the Home Office, NTAC and the relevant communications service provider. As the level of security is based on a number of factors and is a balance of four broad areas, there is no single minimum security standard. However, all communications service providers will be required to follow the key principles of security set out in the paragraphs below. It is open to a communications service provider to put in place alternative controls or mitigations which provide assurance of the security of the data where agreed with the Home Office and NTAC.

8.64 Communications service providers operating under a technical capability notice will provide timely access to NTAC to assess physical, personnel, procedural and information security. NTAC will provide subsequent security advice and guidance to the communications service provider.

Integrity of interception and delivered product

8.65 When interception is authorised and conducted under the Act, checks should be undertaken by the communications service provider at intervals agreed with NTAC to ensure the integrity and security of interception and the delivery of correct product.

8.66 The intercepting agency must be notified of any errors (including breaches) in the interception. NTAC should be notified of any problems or changes to interception capability or the delivery of intercept product.

8.67 The communications service provider must ensure that audit systems are in place to provide assurance that no unauthorised changes have been made to the interception identifiers/factors and to confirm details of those identifiers/factors.

8.68 In the event that checks indicate any problems or changes in relation to the warranted interception, the intercepting agency will advise the communications service provider on any further action that may be required.

Principles of data security, integrity and disposal of systems

Legal and regulatory compliance

8.69 All interception systems and practices must be compliant with relevant legislation.

8.70 All systems and practices must comply with any security policies and standards in place in relation to the interception of communications. This may include any policies and standards issued by the Home Office or NTAC. These further requirements are unlikely to be publicly available as they may contain specific details of security infrastructure or practices, disclosure of which could create additional security risks.

Information security policy & risk management

8.71 Each communications service provider must develop a security policy. This policy document should describe the internal security organisation, the governance and authorisation processes, access controls, necessary training, the allocation of security responsibilities, and policies relating to the security and integrity of interception capabilities and information related to warranted interception. Each communications service provider must also develop security operating procedures. A communications service provider can determine whether this forms part of, or is additional to, wider company policies.

8.72 The security policy document and security operating procedures should be reviewed regularly to ensure they remain appropriate

8.73 Each communications service provider must identify, assess and treat all information security risks, including those which relate to arrangements with external parties.

Human Resources Security

8.74 Communications service providers must clearly identify roles and responsibilities of staff, ensuring that roles are appropriately segregated to ensure staff only have access to the information necessary to complete their role. Access rights and permissions assigned to users must be revoked on termination of their employment. Such rights and permissions must be reviewed and, if appropriate, amended or revoked when staff move roles within the organisation.

8.75 Staff with access to intercepting systems and sensitive information related to warranted interception should be subject to an appropriate level of security screening. The Government sponsors and manages security clearance for certain staff working within a communications service provider to ensure the company's compliance with obligations under this legislation. Communications service providers must ensure that these staff have undergone relevant security training and have access to security awareness information.

8.76 All persons who may have access to intercepted content, or need to see any reporting in relation to it, must be appropriately vetted. On an annual basis, managers must identify any concerns that may lead to the vetting of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed.

8.77 Where it is necessary for an officer of an intercepting agency or a member of NTAC staff to disclose information related to warranted interception to a communications service provider operating under a technical capability notice, it is the former's responsibility to ensure that the recipient has the necessary security clearance.

Maintenance of Physical Security

8.78 There should be appropriate security controls in place to prevent unauthorised access to sensitive information. Access to the locations where the systems are both operated and hosted must be controlled such that access is limited to those with the relevant security clearance and permissions.

8.79 Equipment used to intercept communications must be sanitised and securely disposed of at the end of its life[25].

Operations management

8.80 Interception systems should be subject to a documented change management process, including changes to third party suppliers, to ensure that no changes are made to systems without assessing the impact on the security of interception product.

8.81 Communications service providers must also put in place a patching policy to ensure that regular patches and updates are applied to any interception capabilities or support systems as appropriate. Such patches and updates will include anti-virus, operating systems, application and firmware. The patching policy including timescale in which patches must be applied, must be agreed with the Home Office and NTAC.

8.82 Communications service providers should ensure that, where encryption is in place in interception systems, any encryption keys are subject to appropriate controls, in accordance with the appropriate security policy.

8.83 In order to maintain the integrity and security of interception and the delivery of product, communications service providers must ensure that data being processed is validated against agreed criteria.

8.84 Network infrastructure, services, media, and system documentation must be stored and managed in accordance with the security policy and an inventory of all assets should be maintained together with a clear identification of their value and ownership. All assets must be clearly labelled.

8.85 Interception systems, and their use, should be monitored and all audit logs compiled, secured and reviewed by the communications service provider security manager at appropriate intervals. These should be made available for inspection by NTAC as required. Communications service providers must demonstrate audit and compliance procedures in line with ISO27000.

8.86 Technical vulnerabilities must be identified and assessed through an independent IT Health Check (ITHC) which must be conducted annually. The scope of the Health Check must be agreed with NTAC.

Access Controls

8.87 Communications service providers must ensure that registration and access rights, passwords and privileges for access to dedicated interception systems and associated documentation are managed in accordance with their security policy. They must also ensure that users understand and formally acknowledge their security responsibilities.

[25] Please see 8.92 for further details on the disposal of interception systems.

8.88 Access to operating systems must be locked down to an appropriate standard and any mobile computing (i.e. offsite access to communications service provider systems from non-secure locations) must be subject to appropriate policies and procedures if permitted. Accordingly any remote access for diagnostic, configuration and support purposes must be controlled.

8.89 Access should be provided to relevant oversight bodies where necessary for them to carry out their functions.

Management of incidents

8.90 Communications service providers must put in place clear incident management processes and procedures, including an escalation path to raise issues to senior management and NTAC. Any breaches under relevant legislation should be notified in accordance with those provisions.

8.91 Systems must enable the collection of evidence (e.g. audit records) to support investigation into any breach of security.

Additional requirements relating to the disposal of systems

8.92 The legal requirement to ensure deleted data is impossible to access must be taken into account when disposing of any system, or component of a system, which reaches the end of its service life.

8.93 If the equipment is to be re-used, it must be securely sanitised by means of overwriting using a Government-approved product. If the equipment is not to be re-used immediately, it must be securely stored in such a way that it may only be re-used or disposed of appropriately.

8.94 If the equipment is to be finally disposed of, it must be securely sanitised by means of physical destruction by a Government-approved supplier.

8.95 Sanitisation or destruction of interception identifiers/factors must include retained copies for back-up and recovery, and anything else that stores duplicate data within the communications service provider's system, unless retention of this is otherwise authorised by law.

9. Safeguards (including sensitive professions)

9.1 All content intercepted under the authority of an interception warrant and any secondary data must be handled in accordance with safeguards which the Secretary of State has approved in line with the duty imposed on him or her by the Act. These safeguards are made available to the Investigatory Powers Commissioner, and they must meet the requirements of section 51 for Part 2 warrants and section 140 for Part 6 warrants. Breaches of these safeguards must be reported to the Investigatory Powers Commissioner as agreed with him or her. The intercepting agencies must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, the agencies must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

9.2 Sections 51 and 140 of the Act require that disclosure, copying and retention of intercepted content is limited to the minimum necessary for the authorised purposes. Sections 46(3) and 132(3) of the Act provides that something is necessary for the authorised purposes if the intercepted content:

- Is, or is likely to become, necessary for any of the purposes set out in section 20 for targeted warrants or 129(1)(b) and 129(2) for bulk warrants – namely, in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well-being of the UK[26];
- Is necessary for facilitating the carrying out of the functions under the Act of the Secretary of State, the Scottish Ministers or the person to whom the warrant is addressed;
- Is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal;
- Is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of him or her by his or her duty to secure the fairness of the prosecution; or
- Is necessary for the performance of any duty imposed by the Public Record Acts 1967.

[26] Intercepted content obtained for one purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained for another. This is provided for under s19 of the Counter Terrorism Act.

9.3 Section 55 of the Act sets out the meaning of "excepted disclosure" and the circumstances in which disclosure made in relation to a warrant is permitted. This includes when a disclosure is made, not only in relation to a particular warrant but in relation to interception warrants in general. This includes provision for communications service providers to be able to publish information in relation to the number of warrants they have given effect to. In order to ensure that this does not reveal sensitive information that could undermine the ability of the security and intelligence and law enforcement agencies to do their job, further information on the way in which this information can be published is set out in regulations. The regulations make clear that statistical information can be published on the number of warrants that a communications service provider has given effect to within a specified range rather than the exact number.

9.4 Section 55(4)(a) provides for disclosure by a lawyer for the purpose of legal proceedings. Section 55(4)(b) provides for disclosure by a legal adviser or their client or representatives in connection with giving advice about the operation of part 2, chapter 1 of the Investigatory Powers Act 2016 or part 1, chapter 1 of the Regulation of Investigatory Powers Act 2000. However, these exceptions do not override the prohibition on disclosure for the purpose of proceedings in section 53. The effects of these sections is also that any disclosure to a lawyer by the person listed in section 54(3) must either be for the purposes in section 55(4)(b) or be permissible under one of the other 'Heads' set out in section 55. In addition to this, disclosure may be subject to other duties of confidentiality, for example, from contractual or confidential agreements. In particular, the exceptions in section 55 do not override duties imposed by the Official Secrets Act 1989 or other requirements of vetting. In practice, this means that any disclosure to or by lawyers under this section will require reasonable measures to be taken to ensure that sensitive material is properly protected.

Dissemination of intercepted content

9.5 Intercepted content and secondary data will need to be disseminated both within and between agencies, as well as to consumers of intelligence, where necessary in order for action to be taken on it. The number of persons to whom any of the intercepted content is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out in section 51(3) of the Act for targeted interception warrants, and 140(3) of the Act for bulk interception warrants. 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 have not been appropriately vetted and also by the need-to-know principle: intercepted content 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 or she needs to know about the intercepted content to carry out those duties. In the same way, only so much of the intercepted content may be disclosed as the recipient needs. For example, if a summary of the intercepted content will suffice, no more than that should be disclosed.

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

9.7 Section 55(2) sets out that disclosures may be authorised by the warrant, by the person to whom the warrant is addressed or by the terms of any requirement to provide assistance in giving effect to a warrant. If the issuing authority or the person to whom the warrant is addressed intends to authorise a disclosure under this section they must first consider the safeguards set out in section 51 of the Act and paragraphs 9.9-9.13 of this Code.

9.8 Sections 52 and 141 of the Act stipulate that where intercepted content is disclosed to the authorities of a country or territory outside the UK, the appropriate UK intercepting agency must ensure that intercepted content is only handed over to overseas authorities if the following requirements are met:

- It appears to the UK intercepting agency that the requirements corresponding to the requirements in section 51(2) and (5) for targeted warrants, or 140(2) for bulk warrants (relating to minimising the extent to which content is disclosed, copied, distributed and retained) will apply to the extent that the UK intercepting agency considers appropriate; and

- Restrictions are in force which would prevent, to such extent as the appropriate UK intercepting agency considers appropriate, the doing of anything in, for the purpose of or in connection with any proceedings outside the UK which would result in an unauthorised disclosure.

9.9 The intercepted content must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed.

Copying

9.10 Intercepted content may only be copied to the extent necessary for the authorised purposes set out in sections 51(3) and 140(3) of the Act. Copies include not only direct copies of the whole of the intercepted content, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which includes the identities of the persons to or by whom the intercepted content 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

9.11 Intercepted content 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 vetting. This requirement to store intercept product securely applies to all those who are responsible for handling it, 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 have with the Government before being asked to give effect to a warrant.

9.12 Individuals should be granted access only where it is required to carry out their function in relation to one of the authorised purposes set out in section 51(3) of the Act.

9.13 In particular, each intercepting agency must apply the following protective security measures:

- Physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- A security vetting regime for personnel which is designed to provide assurance that those who have access to this content are reliable and trustworthy.

Destruction

9.14 Intercepted content, and all copies, extracts and summaries which can be identified as the product of an interception, must be marked for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes. In this context, this means taking such steps as might be necessary to make access to the data impossible. If such intercepted content is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 51(3) or, in the case of a bulk warrant, section 140(3) of the Act.

9.15 Where an intercepting agency undertakes interception under a bulk warrant and receives unanalysed intercepted content and/or secondary data from interception under that warrant, the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the IPC. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular intercepting agency on the basis that continued retention of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue.

9.16 Any collateral material that has been acquired over the course of a testing or training exercise should be destroyed as soon as reasonably possible following the conclusion of the testing or training.

Safeguards applicable to the handling of intercepted content obtained as a result of a request for assistance

9.17 Section 9 provides that the Secretary of State must ensure that no request for interception of communications sent by or intended for an individual who the person making the request believes will be in the in the British Islands should be made on or behalf of a person in the United Kingdom unless a targeted interception warrant or targeted examination warrant has been issued under Chapter 1 of Part 2. This means that when an intercepting agency asks an overseas authority to carry out (on its behalf) interception on a person in the UK which the overseas authority would not otherwise have been carrying out, the intercepting agency must have an interception warrant in place. Where intercepted communications content or secondary data is obtained by a UK intercepting agency as a result of a request to an international partner to undertake interception on its behalf, the communications content and secondary data must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under the Act.

Rules for requesting and handling unanalysed intercepted communications content and secondary data from a foreign government

Application of this chapter

9.18 This chapter applies to those intercepting agencies that undertake bulk interception under a Part 6 warrant.

Requests for assistance other than in accordance with an international mutual assistance agreement

9.19 A request may only be made by an intercepting agency to the government of a country or territory outside the UK for unanalysed intercepted communications content (and secondary data), otherwise than in accordance with an international mutual assistance agreement, if either:

- A relevant interception warrant under the Act has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular communications because they cannot be obtained under the relevant interception warrant issued under the Act and it is necessary and proportionate for the intercepting agency to obtain those communications; or
- Making the request for the particular communications in the absence of a relevant interception warrant issued under the Act does not amount to a deliberate circumvention of the Act or otherwise frustrate the objectives of the Act (for example, because it is not technically feasible to obtain the communications via interception under the Act), and it is necessary and proportionate for the intercepting agency to obtain those communications.

9.20 A request falling within the second bullet of the above paragraph may only be made in exceptional circumstances and must be considered and decided upon by the Secretary of State personally. The subject of such a request must not be an individual who the person making the request believes will be in the in the British Islands.

9.21 For these purposes, a "relevant interception warrant under the Act" means one of the following: (i) a targeted interception warrant in relation to the subject at issue; (ii) a bulk interception warrant and one or more operational purposes for which the selection for examination of the subject's communications is considered necessary, together with a targeted examination warrant for individuals who the person making the request believes will be in the in the British Islands; or (iii) a bulk interception warrant and one or more operational purposes for which the selection for examination of the subject's communications is considered necessary (for other individuals).

Safeguards applicable to the handling of unanalysed intercepted communications from a foreign government

9.22 If a request falling within the second bullet of paragraph 9.19 is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be selected for examination by the intercepting agency according to any factors referable to an individual who is known for the time being to be in the British Islands unless the Secretary of State has personally considered and approved the selection for examination of those communications by reference to such factors.[27]

9.23 Where intercepted communications content or secondary data are obtained by the intercepting agencies as set out in paragraph 9.19, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content[28] and secondary data[29] must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under the Act.

9.24 All requests in the absence of a relevant interception warrant issued under the Act to the government of a country or territory outside the UK for unanalysed intercepted communications (and secondary data) will be notified to the Investigatory Powers Commissioner.

[27] All other requests within paragraph 9.18 (whether with or without a relevant interception warrant under the Act) will be made for material to, from or about specific selectors (relating therefore to a specific individual or individuals). In these circumstances the Secretary of State will already therefore have approved the request for the specific individual(s).

[28] Whether analysed or unanalysed.

[29] Whether or not those data are associated with the content of communications.

Collateral intrusion

9.25 Consideration should be given to any interference with the privacy of individuals who are not the subject of the intended interception. An application for a targeted interception warrant or a targeted examination warrant should state whether the interception or selection for examination is likely to give rise to a degree of collateral infringement into privacy. A person applying for an interception warrant must also consider appropriate measures, including, for example, the use of automated systems, to reduce the extent of collateral intrusion. Where it is possible to do so, the application should specify those measures. These circumstances and measures will be taken into account by the Secretary of State and Judicial Commissioner when considering an application for the issue of a targeted interception warrant or a targeted examination warrant made under section 15 of the Act. Should an interception operation reach the point where individuals other than the subject of the authorisation are identified as investigative targets in their own right, for example when intercepting the landline of a house with more than one occupant, consideration should be given to applying for separate warrants covering those individuals.

Confidential information and sensitive professions

9.26 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. This includes where the communications contain information that is legally privileged; confidential journalistic material; where interception might involve communications between a medical professional or Minister of Religion and an individual relating to the latter's health or spiritual welfare; or where communications between a Member of Parliament and another person on constituency business may be involved.

9.27 Section 26 of the Act provides additional protection for members of either House of Parliament, the Scottish Parliament, the National Assembly for Wales, the Northern Ireland Assembly or of the European Parliament elected for the UK. The Prime Minister must explicitly authorise any case where it is necessary to issue a targeted interception warrant or a targeted examination warrant in respect of the communications of a Member of Parliament, apart from those approved by Scottish Ministers. The Prime Minister must also explicitly approve any decision made to renew such a warrant (section 31(7) of the Act).

9.28 In a case where section 26 applies in relation to making a major modification, the interception or selection for examination must be approved by a Judicial Commissioner The Prime Minister must explicitly approve any decision made to renew such a warrant (section 31(7) of the Act). The Prime Minister must also approve any application to select for examination the communications of an MP obtained under a bulk interception warrant.

9.29 Particular consideration must also be given to the interception of communications or the examination of content that involves confidential journalistic material, confidential personal information, or communications between a Member of Parliament and another person on constituency business.

9.30 Confidential journalistic material includes content 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.

9.31 Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, where the content in question relates to his or her 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 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.

9.32 Spiritual counselling is defined as conversations between an individual and a Minister of Religion acting in his or her 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.

9.33 Where the intention is to acquire confidential personal information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential personal information is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to whether special handling arrangements are required within the intercepting agency.

9.34 Content which has been identified as confidential information should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes set out in section 51(3). It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.

9.35 Where confidential information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the content takes place.

9.36 Any case where confidential information is retained should be notified to the Investigatory Powers Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any content which has been retained should be made available to the Commissioner on request.

9.37 The safeguards set out above also apply to any content obtained under a bulk interception warrant (see chapter 6) which is selected for examination and which constitutes confidential information and is retained for an intelligence purpose.

Communications subject to legal privilege

9.38 Section 98 of the Police Act 1997 describes those matters that are subject to legal privilege in England and Wales. In Scotland, those matters subject to legal privilege contained in section 412 of the Proceeds of Crime Act 2002 should be adopted. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

9.39 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, for example, the professional legal adviser is intending to hold or use the information for a criminal purpose. But privilege is not lost if a professional legal adviser 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.

9.40 For the purposes of this Code, any communication between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the communication does not form part of a professional consultation of the lawyer, or there is clear and compelling evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the communications are subject to legal privilege or over whether communications are not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from a legal adviser within the relevant intercepting agency.

9.41 Section 27 of the Act provides special protections for legally privileged communications. Intercepting such communications (or examining intercepted content which contains such communications and has been obtained under a bulk interception warrant) is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR as well as engaging Article 8. The interception of communications subject to legal privilege (whether deliberately obtained or otherwise) is therefore subject to additional safeguards under this code as set out at paragraphs 9.42 – 9.45 below. The guidance set out below may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to other content which has been sought.

Application process for warrants that are likely to result in acquisition of legally privileged communications

9.42 Where interception under a targeted warrant or the examination of intercepted content obtained under a bulk warrant is likely to result in a person acquiring communications subject to legal privilege, the application should include, in addition to the reasons why it is considered necessary for the interception or examination to take place, an assessment of how likely it is that communications which are subject to legal privilege will be intercepted or examined. In addition, it should state whether the purpose (or one of the purposes) of the interception or examination is to obtain privileged communications. Where the intention is not to acquire communications subject to legal privilege, but it is likely that such communications will nevertheless be acquired during targeted interception or examination of intercepted content collected under a bulk warrant, that should be made clear in the warrant application, or at the point of selection for examination, and the relevant agency should confirm that any inadvertently obtained communications that are subject to legal privilege will be treated in accordance with the safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to the communications subject to legal privilege.

9.43 Where the intention is to acquire legally privileged communications, the Secretary of State will only issue a targeted warrant under section 15 if he or she, and the Judicial Commissioner are satisfied that there are exceptional and compelling circumstances that make the authorisation necessary. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb or in the interests of national security, and the interception is reasonably regarded as likely to yield intelligence necessary to counter the threat.

Example

An intelligence agency may need to deliberately target legally privileged communications where the legal consultation might yield intelligence that could prevent harm to a potential victim or victims. For example, if they have intelligence to suggest that an individual is about to conduct a terrorist attack and the consultation may reveal information that could assist in averting the attack (e.g. by revealing details about the location and movements of the individual) then they might want to target the legally privileged communications.

9.44 Further, in considering any such application, the Secretary of State and Judicial Commissioner must be satisfied that the proposed conduct is proportionate to what is sought to be achieved. In particular the Secretary of State and Judicial Commissioner must consider whether the purpose of the proposed interception could reasonably be served by obtaining non-privileged information. 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 discretion on whether a warrant should continue to have effect.

9.45 Where there is a renewal application in respect of a warrant which has resulted in the obtaining of legally privileged content, that fact should be highlighted in the renewal application.

9.46 In a case where section 27 (items subject to legal privilege) applies in relation to making a major modification, the warrant must be approved by a Judicial Commissioner

Selection for examination of legally privileged content obtained under a bulk interception warrant: requirement for prior approval by independent senior official

9.47 In line with section 143 of the Act, where the content of communications intercepted under a bulk interception warrant are to be selected for examination according to a factor that is intended to, or is likely to result in, acquiring communications subject to legal privilege, the enhanced procedure described at paragraph 9.42 and 9.43 applies. This only applies where the individual is outside the British islands, otherwise the relevant targeted examination warrant application would address these considerations as described in paragraph 9.42.

9.48 An authorised person in an intercepting agency must notify a senior official[30] before using a factor to select any bulk intercepted content for examination, where this will, or is likely to, result in the acquisition of legally privileged communications. The notification must address the same considerations as described in paragraph 9.40. The senior official, who must not be a member of the intercepting agency to whom the bulk interception warrant is addressed, must in any case where the intention is to acquire communications subject to legal privilege, apply the same tests and considerations as described in paragraphs 9.42 and 9.43. The authorised person is prohibited from accessing the content until he or she has received approval from the senior official authorising the selection of communications subject to legal privilege.

9.49 In the event that privileged communications are inadvertently and unexpectedly selected for examination (and where the enhanced procedure in paragraph 9.45 has consequently not been followed), any content so obtained must be handled strictly in accordance with the provisions of this chapter. No further privileged communications may be intentionally selected for examination by reference to that factor unless approved by the senior official as set out in paragraph 9.47.

Lawyers' communications

9.50 Where a lawyer, acting in this capacity, is the subject of a targeted interception warrant or a targeted examination warrant or whose communications have been selected for examination in accordance with section 143, it is possible that a substantial proportion of the communications which will be intercepted, examined or selected will be between the lawyer and his or her client(s) and will be subject to legal privilege. Therefore, in any case where the subject of a targeted interception warrant or a targeted examination warrant is known to be a lawyer acting in this capacity where it is intended that a lawyer's communications are to be selected for examination, the application or notification must be made on the basis that it is likely to acquire communications subject to legal privilege and the provisions in this chapter will apply, as relevant. This paragraph does not prevent an application being made on the grounds that the lawyer is under investigation for serious criminal offences.

[30] Senior official is defined in section 145

9.51 Any such case should also be notified to the Investigatory Powers Commissioner during his or her next inspection and any content which has been retained should be made available to the Commissioner on request.

Handling, retention and deletion

9.52 In addition to safeguards governing the handling and retention of intercepted content as provided for in section 51 of the Act, officials who examine intercepted communications should be alert to any intercepted content which may be subject to legal privilege.

9.53 Where it is discovered that privileged content has been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain it for one or more of the authorised purposes set out in section 51(3). If not, the content should be securely destroyed as soon as possible.

9.54 Content which has been identified as legally privileged should be clearly marked as subject to legal privilege. Such content should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes set out in section 51(3). It must be securely destroyed when its retention is no longer needed for those purposes. If such content is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.

Dissemination

9.55 Content subject to legal privilege must not be acted on or further disseminated unless a legal adviser has been consulted on the lawfulness (including the necessity and proportionality) of such action or dissemination.

9.56 The dissemination of legally privileged content to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates, including law enforcement authorities. In this regard civil proceedings includes all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Prosecution Service lawyer nor any other prosecuting authority lawyer with conduct of a prosecution should have sight of any communications subject to legal privilege, held by the relevant intercepting agency, with any possible connection to the proceedings. In respect of civil proceedings, there can be no circumstances under which it is proper for any intercepting agency to have sight of or seek to rely on communications subject to legal privilege in order to gain a litigation advantage over another party in legal proceedings.

9.57 In order to safeguard against any risk of prejudice or accusation of abuse of process, public authorities must also take all reasonable steps to ensure that lawyers or other officials with conduct of legal proceedings should not see legally privileged communications relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the intercepting agency must seek independent advice from Counsel and, if there is assessed to be a risk that sight of such content could yield a litigation advantage, the direction of the Court must be sought.

Reporting to the Commissioner

9.58 In those cases where communications identified as being legally privileged have been intercepted or, in the case of communications intercepted in bulk, selected for examination and retained, the matter should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any content that is still being retained should be made available to him or her on request, including detail of whether that content has been disseminated.

10. Record keeping and error reporting

Records

10.1 Records must be available for inspection by the Investigatory Powers Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part 8 of the Act, to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates, particularly where continuing conduct is alleged. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to five years. The following information relating to all warrants for interception should be centrally retrievable for at least three years:

- All applications made for targeted interception warrants and bulk interception warrants, and applications made for the renewal of such warrants;
- All warrant Instruments, associated schedules, renewal instruments and copies of modification applications (if any);
- Where any application is refused, the grounds for refusal as given by the Secretary of State or Judicial Commissioner;
- The dates on which interception started and stopped.

10.2 Records should also be kept of the arrangements for securing that only content which has been determined as necessary is, in fact, read, looked at or listened to. Records should be kept of the arrangements by which the requirements of section 51(4) (minimisation of copying and distribution of intercepted content) and section 51(5) (destruction of intercepted content) are to be met.

10.3 Records should also be kept by the relevant Department of State of the warrant authorisation process. This will include:

- All advice provided to the Secretary of State to support his/her consideration as to whether to issue or renew the targeted interception warrant or bulk interception warrant; and
- Where the issuing of any application is not approved by the Judicial Commissioner, the grounds for refusal as given by the Judicial Commissioner and any associated advice / applications to the Investigatory powers Commissioner if there is an appeal.

10.4 Each relevant intercepting agency must also keep a record of the information below for every calendar year to assist the Investigatory Powers Commissioner in carrying out his statutory functions.

Targeted Warrants

10.5 For the purposes of these record keeping requirements a targeted warrant should be taken as referring to a targeted interception warrant, targeted examination warrant or mutual assistance warrant, issued under Part 2 of the Act. In recording this information, each relevant intercepting agency must keep records for each of these three individual categories of warrant:

- The number of applications made by or on behalf of the intercepting agency for a targeted warrant.
- The number of applications for a targeted warrant that were refused by a Secretary of State.
- The number of applications for a targeted warrant that were refused by a Judicial Commissioner.
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse a targeted warrant.
- The number of targeted warrants issued by the Secretary of State and approved by a Judicial Commissioner.
- The number of targeted warrants authorised by the Secretary of State and issued urgently by a senior official.
- The number of targeted warrants authorised by the Secretary of State and issued urgently by a senior official that were subsequently refused by a Judicial Commissioner.
- The number of renewals to targeted warrants that were made.
- The number of targeted warrants that were cancelled.
- The number of targeted warrants extant at the end of the calendar year.

10.6 For each targeted warrant issued by the Secretary of State and approved by a Judicial Commissioner (including warrants issued and approved in urgent cases), the relevant public authority must also keep a record of the following:

- The section 20 purpose(s) specified on the warrant.
- The details of major and minor modifications made to the warrant.

Bulk Interception Warrants

10.7 Each relevant intercepting agency must keep a record of the following information to assist the Investigatory Powers Commissioner in carrying out his statutory functions:

- The number of applications made by or on behalf of the intercepting agency for a bulk interception warrant.
- The number of applications for a bulk interception warrant that were refused by a Secretary of State.
- The number of applications for a bulk interception warrant that were refused by a Judicial Commissioner.
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse a bulk interception warrant.
- The number of bulk interception warrants issued by the Secretary of State and approved by a Judicial Commissioner.
- The number of renewals to bulk interception warrants that were made.
- The number of bulk interception warrants that were cancelled.
- The number of bulk interception warrants extant at the end of the year.

10.8 For each bulk interception warrant issued by the Secretary of State and approved by a Judicial Commissioner, the relevant public authority must also keep a record of the following:

- The section 130(1)(b) and section 130(2) purpose(s) specified on the warrant.
- The details of modifications made to add, vary or remove an operational purpose from the warrant.
- The number of modifications made to add or vary an operational purpose that were made on an urgent basis.
- The number of modifications made to add or vary an operational purpose (including on an urgent basis) that were refused by a Judicial Commissioner.
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse to modify a bulk interception warrant.

10.9 These records must be sent in written or electronic form to the Investigatory Powers Commissioner, as determined by him. Guidance on record keeping will be issued by the Investigatory Powers Commissioner. Guidance may also be sought from the Commissioner by intercepting authorities.

Errors

10.10 This section provides information regarding errors, which are not considered to meet the threshold of the offences detailed in Chapter 3 of this code.

10.11 A relevant error which must be reported to the Investigatory Powers Commissioner is defined in section 207(9) of the Act as an error:

a. By a public authority complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner; and

b. Of a description identified for this purpose in a Code of Practice or in guidance provided by the Commissioner.

10.12 An error can only occur after interception of communications has commenced. Such an error can occur only where:

- Unauthorised interception of communications within the meaning of section 4 of the Act has or is believed to have occurred and product has been diverted or recorded so as to be made available to a person subsequently[31]

- There has been material failure to adhere to the arrangements in force under section 51 of the Act relating to material obtained by targeted interception, or the safeguards relating to material obtained by bulk interception contained in sections 140, 141 or 142 of the Act.

- Interception of communications has taken place resulting in collection of communications that would not have occurred but for conduct or an omission of the part of a member of the public authority or other such person assisting to give effect to a warrant.

10.13 Situations may arise where an interception warrant under Part 2 of the Act has been obtained or modified as a result of the relevant agency having been provided with a communications address – for example, by another domestic intelligence agency, police force or communications service provider – which later proved to be incorrect, due to an error on the part of the person providing the communications address, but on which the relevant agency acted in good faith. Whilst these actions do not constitute a relevant error on the part of the relevant agency, such occurrences should be brought to the attention of the Commissioner.

[31] Unauthorised interception is a failure to have in place a warrant in accordance with the provisions of the Act where one would have been required to render the activity lawful

10.14 Proper application of the Investigatory Powers Act and thorough procedures for operating its provisions, including for example the careful preparation and checking of warrants, modifications and schedules, should reduce the scope for making errors whether by the public authority, Communications service provideror other persons assisting in giving effect to the warrant.

10.15 Any failure by the public authority or such other persons providing assistance to apply correctly the process set out in this code will increase the likelihood of an error occurring.

10.16 All relevant errors must be reported to the Commissioner. Errors can have very significant consequences on an affected individual's rights.

10.17 Reporting of errors will draw attention to those aspects of the interception process that require further improvement to eliminate errors and the risk of undue interference with any individual's rights.

10.18 This section of the code cannot provide an exhaustive list of possible errors. Examples could include:

- Unauthorised interception of communications within the meaning of section 4 of the Act has or is believed to have occurred and product has been diverted or recorded so as to be made available to a person subsequently.[32]
- interception of communications has taken place that would not have occurred but for conduct or an omission of the part of a member of the relevant agency or communications service provider;
- human error, such as incorrect transposition of communications addresses or identifiers from an application to a warrant or schedule which leads to the wrong intercepted content or data being intercepted;
- warranted interception has taken place on a communications address but the communications do not in the event relate to the intended persons or premises where information available at the time of seeking a warrant could reasonably have indicated this.
- a material failure to adhere to the arrangements in force under section 51 of the Act relating to content obtained by targeted interception, or the safeguards relating to content obtained by bulk interception contained in sections 140, 141 or 142 of the Act. For example:
    - over-collection caused by software or hardware errors;
    - unauthorised selection / examination of communications;
    - unauthorised or incorrect disclosure of intercepted content or data (e.g. a communications service provider misdirecting product to the incorrect public authority).
    - failure to effect the cancellation of an interception.

[32] Unauthorised interception is a failure to have in place a warrant in accordance with the provisions of the Act where one would have been required to render the activity lawful

10.19 When an error has occurred, the public authority or other person which made the error (i.e. the communications service provider) must notify the Investigatory Powers Commissioner ten working days after it has been established by appropriate internal governance processes that an error has occurred. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full.

10.20 If the public authority discovers a communications service provider error they should notify the Investigatory Powers Commissioner and the communications service provider of the error straight away to enable the communications service provider to investigate the cause of the error and report it themselves.

10.21 A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error, the date the intercepting agency first became aware of the possibility of the error, the cause, the amount of intercepted content or secondary data obtained or disclosed, any unintended collateral intrusion, any analysis or action taken, whether the content or data has been retained or destroyed and a summary of the steps taken to prevent recurrence. Wherever possible, technical systems should incorporate functionality to minimise errors. A senior person within that organisation must undertake a regular review of errors.

10.22 The Commissioner will keep under review the scope and nature of errors and issue guidance as necessary, including guidance on the format of error reports.

Serious errors

10.23 In circumstances where an error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner must inform the individual concerned, who may make a complaint to the Investigatory Powers Tribunal (see Chapter 13).

10.24 Section 207 of the Act states that the Commissioner must inform a person of any relevant error relating to that person which the Commissioner considers to be a serious error and that it is in the public interest for the person concerned to be informed of the error. In determining any error to be a serious error, the Commissioner must consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

10.25 In deciding whether it is in the public interest for the person concerned to be informed of the error,, the Commissioner must in particular consider:

a. The seriousness of the error and its effect on the person concerned; and

b. the extent to which disclosing the error would be contrary to the public interest or prejudicial to:

- national security
- the prevention or detection of serious crime
- the economic well-being of the United Kingdom; or

- the continued discharge of the functions of any of the intelligence services.

10.26 Before making its decision, the Commissioner must ask the intercepting agency which has made the error to make submissions on the matters concerned.

10.27 When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

11. Disclosure to ensure fairness in proceedings

11.1 Section 51(5) of the Act contains the general rule that intercepted content must be destroyed as soon as its retention is no longer necessary for a purpose authorised under the Act. Section 51(3) specifies the authorised purposes for which retention is necessary.

11.2 This part of the code applies to the handling of intercepted content in the context of criminal proceedings where the content has been retained for one of the purposes authorised in section 51(3) 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 content has not taken place in accordance with section 51(5) and where that content is still in existence after the commencement of a criminal prosecution. In these circumstances, retention will have been considered necessary to ensure that a person conducting a criminal prosecution has the information he or she needs to discharge his or her duty of ensuring its fairness (section 51(3)(d)).

Exclusion of matters from legal proceedings

11.3 The general rule is that neither the possibility of interception, nor intercepted content itself, plays any part in legal proceedings. This rule is set out in section 53 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 Chapter 1 of Part 1 of this Act (or a warrant issued under Chapter 1 of Part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA) or the Interception of Communications Act 1985). This rule means that the intercepted content cannot be used either by the prosecution or the defence. This preserves “equality of arms” which is a requirement under Article 6 of the ECHR.

11.4 Schedule 3 contains a number of tightly-drawn exceptions to this rule. This part of the code provides further detail on the exceptions in paragraph 21, disclosure in criminal proceedings.

Disclosure to a prosecutor

11.5 Paragraph 21(1)(a) of Schedule 3 provides that intercepted content 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.

11.6 This may only be done for the purpose of enabling the prosecutor to determine what is required of him or her by his or her duty to secure the fairness of the prosecution. The prosecutor may not use intercepted content to which he or she is given access under paragraph 21(1)(a) to mount a cross-examination, or to do anything other than ensure the fairness of the proceedings.

11.7 The exception does not mean that intercepted content should be retained against a remote possibility that it might be relevant to future proceedings. The normal expectation is still for the intercepted content to be destroyed in accordance with the general safeguards provided by section 51. The exceptions only come into play if such content has, in fact, been retained for an authorised purpose. Because the authorised purpose given in section 20(2)(b) ("for the purpose of preventing or detecting serious crime") does not extend to gathering evidence for the purpose of a prosecution, content intercepted for this purpose may not have survived to the prosecution stage, as it will have been destroyed in accordance with the section 51(5) safeguards. There is, in these circumstances, no need to consider disclosure to a prosecutor if, in fact, no intercepted content remains in existence.

11.8 Paragraph 21(1)(a) recognises the duty on prosecutors, acknowledged by common law, to review all available content to make sure that the prosecution is not proceeding unfairly. 'Available content' will only ever include intercepted content at this stage if the conscious decision has been made to retain it for an authorised purpose.

11.9 If intercepted content does continue to be available at the prosecution stage, once this information has come to the attention of its holder, the prosecutor should be informed that a warrant has been issued under section 15 of the Act and that content of possible relevance to the case has been intercepted.

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

Disclosure to a judge

11.11 Paragraph 21(1)(b) of Schedule 3 recognises that there may be cases where the prosecutor, having seen intercepted content under paragraph 21(1)(a), will need to consult the trial judge. Accordingly, it provides for the judge to be given access to intercepted content, where there are exceptional circumstances making that disclosure essential in the interests of justice[33].

11.12 This access will be achieved by the prosecutor inviting the judge to make an order for disclosure to him or her alone, under this subparagraph. This is an exceptional procedure; normally, the prosecutor's functions under paragraph 21(1)(a), will not fall to be reviewed by the judge. To comply with section 53(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 fairly.

11.13 The judge may, having considered the intercepted content disclosed to him or her, 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 53(1), 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.

[33] when disclosing in SIAC, disclosure might be made to the Special Advocate but disclosure to the appellant is not permitted.

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

Disclosure to ensure thorough investigations in inquests and inquiries

11.15 Paragraph 21 of Schedule 3 to the Investigatory Powers Act 2016 sets out the circumstances in which disclosure of intercepted content can be made in relation to prosecutors and judges. Paragraph 21(1)(b) of Schedule 3 permits disclosure to a relevant judge alone where the disclosure has been ordered to be made by the judge. This includes cases where a judge has been appointed to sit as Coroner or deputy coroner in an inquest

11.16 Paragraph 24 of Schedule 3 permits disclosure of intercept content to be made to counsel to an inquest and to the solicitor to an inquest. In such cases, counsel or the solicitor must hold current developed vetting (DV) clearance. The disclosure is intended to provide the judge with necessary support in handling sensitive intercept content in inquests.

11.17 Content disclosed to a relevant judge, counsel to an inquest or the solicitor to an inquest will remain subject to the prohibition on disclosure. It cannot be disclosed to other participants in an inquest or to the public. This will allow a judge to consider intercept content and ensure that ECHR compliant inquests can take place.

11.18 Paragraph 24 of Schedule 3 permits disclosure of the existence of intercept content to a coroner in an inquest for the purpose of appointing a relevant judge to the investigation. The disclosure to the Coroner would be that intercept content exists in a given case but it would not include disclosure of the intercept content. Although disclosure is permitted to the Coroner, no further disclosure is permitted by this section. A coroner notified that intercept content may exist in a given case would be prohibited from any further disclosure by section 54(3)(f).

12. Other lawful authority to undertake interception

12.1 Lawful interception can only take place if the conduct has lawful authority (as set out in section 6 of the Act). The Act permits interception of a communication without a warrant in the following circumstances:

- Where the sender and/ or the intended recipient have consented to the interception
- Where it is carried out by the communications service provider for administrative or enforcement purposes; or
- Where it takes place, in relation to any stored communication, under another statutory power being exercised for the purpose of obtaining information or of taking possession of any document or other property. This includes, for example, the obtaining of a production order under Schedule 1 to the Police and Criminal Evidence Act 1984 for stored communications to be produced;

12.2 Interception in accordance with a warrant under sections 15 and 127 of the Act is dealt with under chapters 4, 5, 6 and 7 of this code. Interception without lawful authority may be a criminal offence (see chapter 3 of this code).

12.3 The general rule is that neither the possibility of interception, nor intercepted content itself, plays any part in legal proceedings. This rule is set out in section 53 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.

12.4 Section 46 provides a power for OFCOM to carry out interception in exercising statutory functions relating to the management of the radio frequency network, including in relation to maintaining the security of that network. The work of Ofcom's spectrum engineers, in particular, may involve such interception as part of the function they perform under section 4 of the Wireless Telegraphy Act 2006 of providing advice and assistance to those complaining of interference to the network.

Interception with the consent of one or both parties

12.5 Section 42(1) of the Act authorises the interception of a communication if both the person sending the communication and the intended recipient(s) have given their consent.

12.6 Section 42(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 2 of RIPA or he Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA). Further details can be found in chapter 2 of the Covert Surveillance and Property Interference Code of Practice and in chapter 3 of the Covert Human Intelligence Sources Code of Practice[34], or their RIPSA equivalents.

Interception by providers of postal or telecommunications services

12.7 Section 43 of the Act permits a communications service provider, or a person acting upon their behalf, to carry out interception for the following purposes:

- Purposes connected with the operation of the service. This includes identifying, combating, and preventing anything which could affect a communications service provider's system delivering that service, or could affect devices attached to it;
- Purposes connected with the enforcement of any enactment relating to the use of the communication service
- Blocking and filtering for purposes connected with the restriction of access to content that is unlawful to publish or content which a subscriber has determined is otherwise unsuitable.
- This section permits, for example, a communications service provider offering family friendly filters to restrict its customers from accessing illegal or harmful content.

Interception by businesses for monitoring and record-keeping purposes

12.8 Section 44 of the Act enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept communications for business purposes. Known as the Lawful Business Practice Regulations (LBPRs), these regulations permit the government to protect national security, for example to test and assure the security of their own systems from cyber-attack. They can also be used by the private sector for a broad range of business purposes, including the monitoring of productivity and the detection of offences by employees. The communications systems in question are private networks which the organisation concerned (whether that is a public or private body) has the right to control, and the regulations recognise that an interception warrant is not needed when the information being gathered from the network meets the criteria set out in the regulations.

[34] http://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

12.9 The Government also relies on the regulations for cyber security, to protect critical national infrastructure (CNI) companies, and public sector organisations. They rely on the regulations to undertake on-going protective monitoring of UK organisations in order to learn about and scan for potential cyber-attacks. The regulations are the most effective and timely way to monitor data from vulnerable CNI networks, and the requirement for consent from system controllers ensures that companies are fully aware that their networks are being monitored in the interests of national security, which is the purpose served by detecting a cyber-attack.

Interception in accordance with overseas requests

12.10 Section 50 of the Bill permits a communications service provider to intercept communications in the UK if the request is a lawful order from a valid authority in a country with which the UK has a valid international agreement. The lawful order must meet the requirements of the agreement under which it is submitted, and the conditions set out in secondary legislation must also be met. Communications Service Providers will be free to respond to the request, without an equivalent UK warrant, if these conditions are met. The relevant international agreements to which the UK is party are designated in secondary legislation.

12.11 The Bill provides that the Secretary of State must designate those international agreements to which clause 50 applies. Where a communications service provider is permitted to intercept communications in response to an overseas request, in accordance with an international agreement, the person whose communications are intercepted must be, or be believed to be, outside the UK.

12.12 Section 50 allows the United Kingdom to comply with Article 17 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. This Article allows operators of satellite communications systems to use a ground station in one Member State to facilitate interception using a "service provider" (in practice, a communications service provider which is in a business relationship with the satellite operator) located in another Member State. The "service provider" and the subject of interception are required to be in the same Member State.

Stored communications

12.13 Under section 6(1)(c) of the Act, accessing the contents of a communication stored in or by a system (whether before or after its transmission) constitutes interception. For example, a text message or voicemail on a phone (irrespective of whether it has been read/listened to) is being stored by the system. Access to the system, therefore, would still constitute interception. However, there are other statutory provisions that authorise access to stored communications than an interception warrant. An equipment interference warrant cannot authorise conduct that would constitute the live interception of a communication in the course of its transmission (e.g. live interception of a VoIP call). But section 93(6) sets out that an equipment interference warrant may authorise the obtaining of stored communications i.e. a communication stored in or by a telecommunication system.

12.14 In addition, section 6(1)(c) of the Act makes clear that a person has lawful authority to access stored communications under any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property, or is carried out in accordance with a court order for that purpose.

12.15 There are a number of statutes that are used for the purpose of obtaining stored communications for evidential purposes. Those that are most commonly used by law enforcement agencies include (but are not limited to) the following:

- Powers to search or obtain content under the Police and Criminal Evidence Act 1984
- Powers to search or obtain content under the Proceeds of Crime Act 2002
- Powers to search under the Firearms Act 1968, Protection of Children Act 1978, Theft Act 1968 and the Misuse of Drugs Act 1971

- Powers to examine imported goods under the Customs and Excise Management Act 1979 to examine imported goods

- Powers to examine content under Schedule 7 of the Terrorism Act 2000

12.16 Law enforcement agencies therefore have the ability to access stored communications on devices seized using these powers (such as an email stored on a web-based server or a saved voicemail) during their investigations in order to gather evidence of offences, safeguard children and protect the public

12.17 There will be some instances where law enforcement or security and intelligence agencies may be able to obtain stored communications using a number of provisions contained in different statutes. The decision as to which statute should be used will necessarily be made on a case-by-case basis and will be determined by the nature and status of the investigation.

13. Oversight

13.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ('the Commissioner'), whose remit is to provide comprehensive oversight of the use of the powers contained within Part 2 and Chapter 1 of Part 6 of the Act and adherence to the practices and processes described by this code. By statute the Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work.

13.2 The Investigatory Powers Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The IPC may undertake these inspections, as far as they relate to the IPC's statutory functions, entirely on his or her own initiative or they may be asked to investigate a specific issue by the Prime Minister

13.3 The IPC will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the IPC must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers must, by law, offer all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

13.4 Anyone working for a public authority or communications service provider who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner, who will consider them. In particular, any person who exercises the powers described in the Act or this code must, in accordance with the procedure set out in chapter 10 of this code, report to the Commissioner any action undertaken which they believe to be contrary to the provisions of this code. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority. The Commissioner may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the Investigatory Powers Tribunal (IPT).

13.5 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to an individual who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the individual affected. Further information on errors can be found in chapter 10 of this code. The public body who has committed the error will be able to make representations to the Commissioner before they make their decision on whether it is in the public interest for the individual to be informed.

13.6 The public body who has committed the error will be able to make representations to the IPT before they make their decision.

13.7 The Commissioner must also inform the affected individual of their right to apply to the Investigatory Powers Tribunal (see Complaints chapter for more information on how this can be done) who will be able to fully investigate the error and decide if a remedy is appropriate. The Commissioner must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the national interest. Only the Prime Minister will be able to authorise redactions to the Commissioner's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

13.8 The Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publically available subject to public interest considerations. Public authorities and communications service providers may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce guidance for public authorities on how to apply and use Investigatory Powers. Wherever possible this guidance will be published in the interests of public transparency.

13.9 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: [website for IPC once created]

14. Complaints

14.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against public authority use of investigatory powers and human rights claims against the security and intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

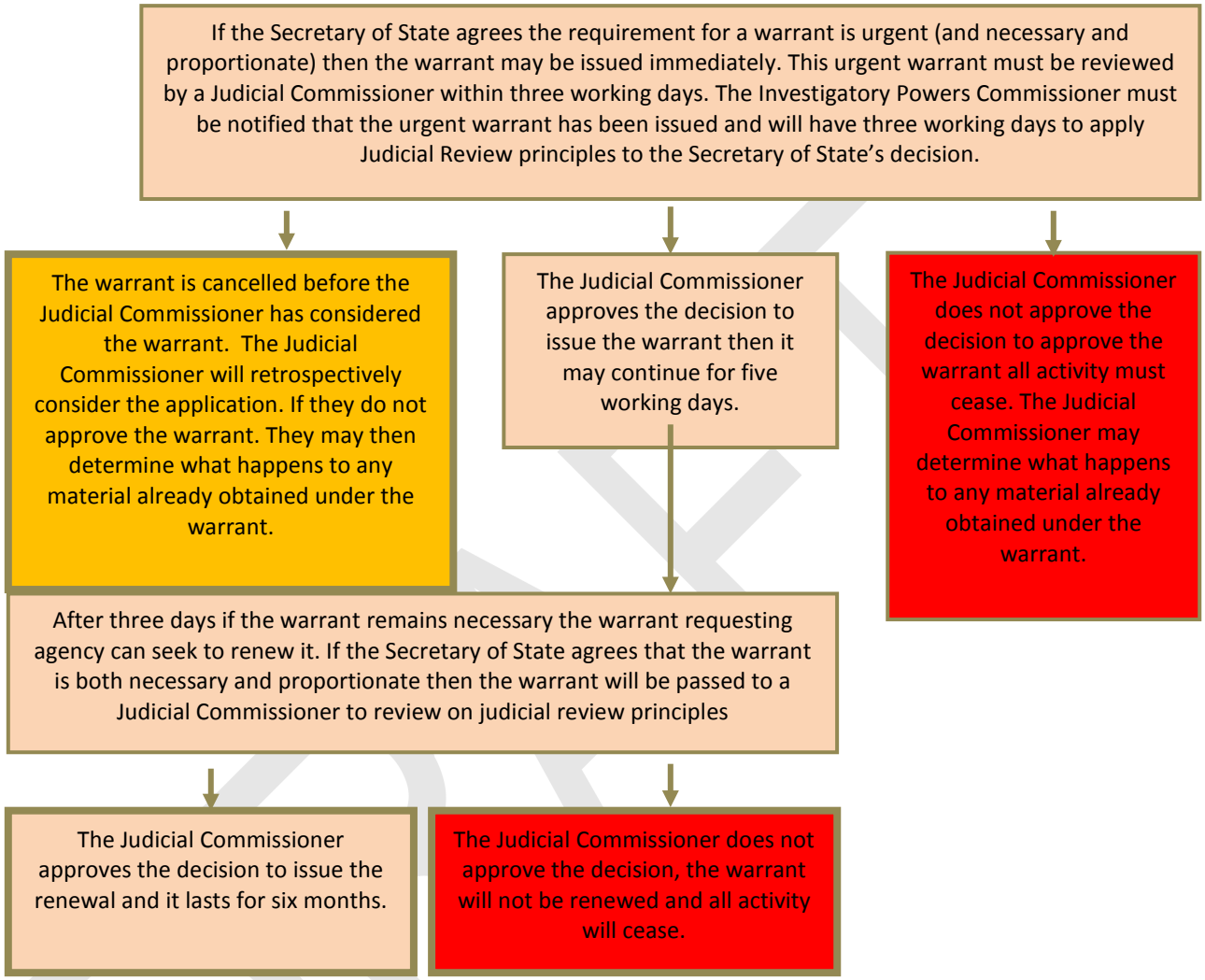
14.2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination.

14.3 This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: http://www.ipt-uk.com. Alternatively information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

14.4 If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

Annex A – Urgent warrant process



This Code of Practice sets out the powers and duties conferred or imposed under Part 2 or Chapter 1 of Part 6 of the Investigatory Powers Act 2016 relating to the lawful interception of communications. It provides guidance on rules and procedures, on record-keeping and on safeguards for handling intercept material.

It provides guidance on:

- procedures to be followed for targeted and bulk interception;
- procedures to be followed for the storage, handling and selection for examination of communications obtained from interception;
- keeping of records, including records of errors; and
- the oversight arrangements in place for interception.

Primarily intended for those public authorities able to apply for the issue of an interception warrant, the code will also be informative to communications service providers' staff involved in the lawful interception of communications and others interested in the conduct of lawful interception of communications.