Home Office

INTERCEPTION OF COMMUNICATIONS

Pursuant to Schedule 7 to the Investigatory Powers Act 2016

[February 2017]

DRAFT Code of Practice

This publication is available at:
www.gov.uk/government/collections/investigatory-powers-bill

Any enquiries regarding this publication should be sent to us at investigatorypowers@homeoffice.gsi.gov.uk

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 and/or the obtaining of secondary data 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, or to the Information Commissioner, it may be taken into account.

1.3. For the avoidance of doubt, the duty to have regard to the Code when exercising functions to which the Code relates exists regardless of any contrary content of an intercepting agency's internal advice or guidance.

2. 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

2.2 Section 4(4) sets out that a "relevant time" in this context means:

- Any time while the communication is being transmitted, and
- Any time when the communication is stored in or by the system (whether before or after its transmission).

What is a communications service provider?

2.3 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.

2.4 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 (wholly or partly) in or controlled from the UK. A postal operator is a person providing a postal service to a person in the UK. These definitions ensure that enforceable 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.

2.5 Section 261(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 electromagnetic energy. The definitions of 'telecommunications service' and 'telecommunications system' in the Act are intentionally broad so that they remain relevant for new technologies.

2.6 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.

2.7 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 be a telecommunications operator if 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.

2.8 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.

2.9 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 secondary data?

2.11 Warrants issued under Chapter 1 of Part 2 and Chapter 1 of Part 6 may authorise the interception of communications and/or the obtaining of secondary data.

2.12 Secondary data comprises system data (as defined in section 235(4)) and identifying data (as defined in section 235(2) and (3)). Secondary data is less intrusive than content but is a broader category of data than communications data (as defined in section 233). For example, it could include technical data such as details of hardware configuration. It could also include information related to a specific communication or piece of content, for example data associated with a photograph, such as the date and location it was taken – though not the photograph itself, as that would still be content.

2.13 **Systems data** is any data that enables or facilitates the functioning of any system or service (but will only be considered secondary data if it is included as part of, attached to or logically associated with the communication). For example, when using an application on a phone there will be data exchanged between the phone and the application server which makes the application work in a certain way. Messages sent between items of network infrastructure to enable the system to manage the flow of communications will also be systems data. Some communications may be comprised entirely of systems data, and will not therefore contain any content.

2.14 **Identifying data** is data which identifies, or assists in identifying, persons, apparatus, systems, services, events and locations. Where this data is comprised in the communication and can be logically separated from the remainder of the communication, and, if it were so separated, would not reveal anything of what might reasonably be considered to the meaning of the communication then the data will be secondary data.

What is meant by the content of a communication?

2.15 The content of a communication is defined in section 261(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.

2.16 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 substance or meaning. It is that meaning that the Act defines as content.

2.17 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.

2.18 There are two exceptions to the definition of content set out in section 261(6). The first is any meaning that could be inferred from the fact of the communication. When a communication is sent, the simple fact of the communication [may] convey some meaning, e.g. it could provide a link between persons or between a person and a service. This exception makes clear that 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.

2.19 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 Content

2.20 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. 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. In the context of postal communications secondary data is limited to system data.

What are overseas-related communications?

2.21 Overseas-related communications are defined in section 136 of the Act as communications sent or received by individuals outside the British Islands. The purpose of the definition is to ensure that bulk interception warrants are foreign focused and cannot have as their main purpose the interception of communications sent between individuals in the British Islands.

[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. Interception can also be lawful in other prescribed circumstances which are set out in sections 44 to 52 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. In the case of stored communications, interception may be lawful if carried out in accordance with a targeted or bulk equipment interference warrant (see the Equipment Interference Code of Practice for further detail), if in the exercise of certain statutory powers (see chapter 12) or if carried out in accordance with a court order.

3.2 Section 3(1) of the Act makes it a criminal offence for a person to intentionally, and without lawful authority, 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. For example where they have unlawfully intercepted a communication but did not do it intentionally;
- But, that person has intercepted a communication at a place in the UK without lawful authority;
- 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 Section 8 of the Act provides a civil means of redress for the sender or intended recipient of a communication. The cause of action arises where a communication is intercepted and the following conditions are met:

- Interception is carried out in the United Kingdom;

- the communication is intercepted in the course of its transmission by means of a private telecommunication system; or

- the communication is intercepted 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.

- the interception is carried out by or with the express or implied consent of a person who has the right to control the operation or use of the private telecommunication system; and

- The interception is carried out without lawful authority.

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 circumstances in which interception is permitted without a warrant.

4.2 Section 15(2)(b) and 136(2)(b) of the Act make clear that interception warrants 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. Secondary data is explained further in Chapter 2 of this code. 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 137(4) and 137(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) provides 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. That 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.

4.4 In no circumstances may a UK intercepting agency ask an international partner to undertake interception on its behalf where the making of the request would amount to a deliberate circumvention of the Act. Paragraph 5.50 provides further information on mutual assistance warrants.

Types of warrants

4.5 Part 2 of the Act provides for three types of warrant which may authorise interception or examination. These are listed in section 15(1) of the Act. Guidance on these warrants is set out in Chapter 5 of this Code. In addition, Chapter 1 of Part 6 provides for bulk interception warrants, guidance on which is provided for in Chapter 6 of this Code.

- A **targeted interception warrant** (see section 15(2) 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. Such a warrant will also authorise any conduct it is necessary to undertake to do what is expressly authorised or required by the warrant. In the case of secondary data only warrants this includes the interception of the content of communications but only so far as it is necessary in order to obtain the secondary data from the communications described in the warrant.

- A **targeted examination warrant** (see section 15(3) 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 cases where content is to be selected for examination on the basis of criteria referable to an individual who the person making the request knows to be in the British Islands at the time that the content is selected for examination. Section 152(5) of the Act provides that where an individual enters or is found to be in the British islands, a senior official may authorise the continued selection of his content using only the existing criteria, and without a targeted examination warrant being in place, 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. Targeted examination warrants may relate to targeted or thematic subjects.

- A **mutual assistance warrant** (see section 15(3) of the Act) authorises or requires the an intercepting authority to either make a request for assistance in accordance with an EU mutual assistance instrument or an international mutual assistance instrument, or to provide assistance in accordance with the same.

- A **bulk interception warrant** (see section 136 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 one or more of the interception of communications, the obtaining of secondary data from the communications described in the warrant, and the selection for examination of the intercepted content or secondary data. A bulk warrant may be issued for the purpose of obtaining secondary data only. A bulk interception warrant will also authorise any conduct it is necessary to undertake to do what is expressly authorised by the warrant. In the case of a warrant authorising only the obtaining of secondary data, this may include the interception of the content of communications only 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.

The intercepting authorities

4.6 There are a limited number of persons who can make an application for an interception warrant, or on whose behalf an application can be made on 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).

[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

- 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.

4.7 Any application for the issue of a warrant must be made on behalf of an intercepting agency.

4.8 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).

4.9 Warrants issued under Part 2 (with the exception of certain mutual assistance warrants in accordance with section 40(2)) and Chapter 1 of Part 6 are issued by the Secretary of State (or a Scottish Minister). 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 5.51.

Necessity and proportionality

4.10 Interception of communications, and the obtaining of secondary data from communications, is likely to involve an interference with a person's rights under the European Convention on Human Rights (ECHR). This is only 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 considers that the warrant 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 263(1) as crime where the offence is one 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.
- 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. The power to issue an interception warrant for the purpose of safeguarding the economic well-being of the UK may 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 5.33 of this document.

4.11 The Secretary of State must also believe that the conduct authorised is proportionate to what is sought to be achieved. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy against the need for the activity in investigative, operational or capability terms. The conduct authorised should offer a realistic prospect of bringing the expected benefit and should not be disproportionate or arbitrary.

4.12 Section 2 of the Act requires a public authority to have regard to the following when issuing, renewing or modifying a warrant under part 2 or 6:

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

- whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant is higher because of the particular sensitivity of that information. This includes whether additional safeguards (as set out in Chapter 9) should apply,

- 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 (including the obligation for a public authority to comply with the Human Rights Act).

4.13 In the case of warrants issued under section 17(2)(c) of the Act for the purposes of testing, training, maintenance or development,, 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. The issuing authority must be clear that it is also required for at least one of the relevant statutory purposes.

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

4.15 The following elements of proportionality should therefore be considered:

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

- What other methods, as appropriate, 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

4.16 As set out in sections 20 (and 21), the fact that the information that would be obtained under the 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 the Scottish Ministers). Intercepting authorities are permitted, for example, 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.

5. Targeted warrants

5.1 This section applies to the three kinds of warrants that may be issued under Part 2 of the Act (as set out at paragraph 4.5). These are:

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

5.2 Responsibility for the issuing of interception warrants rests with the Secretary of State or, in relation to a relevant Scottish application, the Scottish Ministers (see paragraph 5.44 – 5.45). The role of the Judicial Commissioner in approving the decision to issue warrants is explained in paragraph 5.46. Interception, mutual assistance 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 authority.

5.3 Although a warrant will be applied for by one of the intercepting agencies, this does not prevent another intercepting agency assisting them with giving effect to the warrant. For example, agency A might apply for a targeted interception and targeted examination warrant relating to a person, organisation or set of premises. Agency A may be able to carry out the targeted interception warrant on their own but require the assistance of Agency B to give effect to the targeted examination warrant. However, in such circumstances the safeguards which exist (further information can be found in Chapter 9) regarding retention, disclosure and examination of the material that is intercepted or obtained must be complied with regardless of which agency is carrying out the relevant activity.

Subject-matter of targeted warrants

5.4 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 or describe the factors used for identifying the communications to be intercepted or selected for examination (see section 29(8) and (9)).

5.5 Section 17 sets out the subject-matter of targeted warrants and constrains what communications can be described in the warrant, or selected for examination. The subject-matter of interception and examination warrants may be targeted (a particular person or organisation or single set of premises) (section 17(1)) or thematic targeted (section 17(2)).

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

5.6 In many cases,targeted interception, mutual assistance and targeted examination warrants will relate to subjects as set out in 17(1). Section 17(1) warrants are sometimes referred to as "non-thematic" warrants and may relate to:

a) A particular person or organisation, or

b) A single set of premises

5.7 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.[3]

5.8 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 (e.g. the focus of the warrant is the company itself) and section 29(3) will not impose an obligation to name individual employees or workers in the warrant. 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.

5.9 A "set of premises" may include any land, movable structure, vehicle, vessel, aircraft or hovercraft. Where warrants are sought for premises such as vehicles, vessels etc, the communications being sought will relate in many cases to the functioning of the craft itself rather than to the personal communications of those on the craft, and the warrants sought will in many cases be for secondary data.

5.10 In practice, an intercepting authority may need to build intelligence about a legal person or organisation itself, rather than the individuals within the company or organisation. In such circumstances, it may be more appropriate to obtain a warrant against e.g. a company, as opposed to individuals working for it. However, in certain circumstances, such as where a warrant is against a large organisation, the intrusion may be higher than a warrant targeting a small subset of individuals working for that organisation. As such, the intercepting authority will need to justify why it is necessary and proportionate to target the company itself, rather than a limited number of individuals working for that company. Where a warrant relates to a legal person or organisation, or a single set of premises, 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.

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

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 communications transiting 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 communications over 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.

Targeted thematic warrants

5.11 In other cases, interception and examination warrants will relate to subject-matters set out in section 17(2) of the Act. These are sometimes referred to as targeted "thematic" warrants. Thematic warrants, as set out at section 17(2) of the Act, may relate to:

a. A group of persons who share a common purpose or who carry on, or may carry on, a particular activity;

b. 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 purposes of a single investigation or operation; or

c. Testing or training activities.

The requirements that must be met by these kinds of warrants are set out at section 31(4), (5) or (6).

5.12 A thematic warrant may be appropriate where the proposed activity is most suitably dealt with by a thematic subject-matter where the relevant statutory tests are met and where the use of a series of individual warrants is not possible or adds no benefit in terms of accountability and oversight.

Specificity of thematic warrants

5.13 The Act requires, at section 31, that certain additional details must be included in the warrant dependent on the subject-matter(s) of the warrant[4]. For example, a thematic warrant that relates to a group which shares a common purpose must include a description of that purpose as well as the name or description of as many of the persons who form part of that group as it is reasonably practicable to name or describe. An intercepting authority must, when section 31(4) – (6) requires it, name or describe as many of the persons, organisations or sets of premises as is reasonably practicable at the time of the application. Descriptions of persons, organisations or sets of premises must be as granular as reasonably practicable in order to sufficiently enable proper assessment of the proportionality and intrusion involved in the interception.

5.14 In some cases aliases may be used in place of names or descriptions, for example where their real name is not known.

5.15 However, it may not always be reasonably practicable to include the names or descriptions or each and every one of the persons, organisations or sets of premises. Accordingly thematic warrants can be seen to fall into two types, those where it is reasonably practicable to include additional details and those where it is not.

Example of warrant where it is reasonably practicable to individually name those falling within the subject matter of the warrant: *An intercepting authority wishes to intercept the communications of three people for the purposes of an investigation in to human trafficking. The agency applies for a warrant in relation to "more than one person for the purpose of operation X" and those persons are known to be 'Mr A', 'Mr B' and 'Mrs C'. As it is reasonably practicable to do so their names must be included in the warrant at the point of issuing. Once issued the warrant authorises the interception of communications of 'Mr A', 'Mr B' and 'Mrs C' via factors specified within the warrant. Further selectors or further names must be added by modification (see paragraph 5.20) if the agency wishes to undertake further activity.*

Example of warrant where it is <u>not</u> reasonably practicable to specifically name or describe those falling within the subject-matter of the warrant: *An intercepting authority wishes to identify persons accessing terrorist material online. The authority seeks a thematic warrant in relation to more than one person carrying on a particular activity, with the subject-matter of the warrant being "persons accessing the terrorist website 'X'". In such a case, it may not be reasonably practicable to name or describe those persons any further than by a description which is based on their use of website 'X'. Once issued the subject-matter of this warrant is any person known to be accessing the terrorist website 'X' and the interception of any person's communications falling in to that description is lawful. There is no requirement to modify the warrant in accordance with section 34 to add names or descriptions of persons accessing the website.*

[4] As per section 31(4) – (6)

5.16 In the case of the second example, the requirements of the Act would be met as the warrant describes the persons, as far as is reasonably practicable, by reference to them accessing the relevant website. However the warrant application must make clear why the subject-matter is appropriate and why it is not reasonably practicable to name or describe those falling within the relevant subject-matter in any more detail. There is no requirement to modify warrants falling into this category during the currency of the warrant providing those names or descriptions already fall within the subject-matter of the warrant and the description of the persons.

5.17 The practicability of providing individual names or descriptions will need to be assessed on a case by case basis by the intercepting authority making the application and will depend upon, for example, the existing intelligence picture, the scale and pace of operation, the nature of the communications to be intercepted and/or from which secondary data is to be obtained, the nature of the factors and the time constraints of the particular operation.

Authorisation of thematic warrants

5.18 Before issuing a thematic warrant the Secretary of State, or the Scottish Ministers where appropriate, must be satisfied that it is necessary and proportionate to issue it and that the method of naming or describing the subject-matter, and/or additional details in relation to that subject-matter is compliant with the requirements of section 31 of the Act.

5.19 The thematic warrant application, including the necessity and proportionality of the proposed conduct, the assessment of collateral intrusion and the further details provided in relation to the subject-matter of the warrant are provided to assist the Secretary of State and Judicial Commissioner in foreseeing the extent of the interference with privacy authorised by the warrant. The Secretary of State's foresight of the interference with privacy has to be sufficient to allow them to make a proper decision as to the necessity and proportionality of the conduct authorised; otherwise the warrant should not be issued.

Modification of thematic warrants

5.20 Thematic warrants may be modified subject to the provisions in the Act (further detail on modifications, including how they apply to non-thematic warrants, is set out at paragraphs 5.71 to 5.81). The modifications that can be made to a thematic warrant are:

a. Adding, varying or removing the name or description of a person, organisation or set of premises to which the warrant relates, and

b. Adding, varying or removing any factor specified in the warrant in accordance with section 31(8).

5.21 The ability to modify the names or descriptions apply only to thematic warrants. The requirement, to modify these details varies depending on the subject-matter of the original warrant and whether the warrant does or does not provide additional names or descriptions of the persons, organisations or set of premises in relation to the subject matter (as illustrated in the examples in paragraph 5.15).

5.22 For example, for thematic warrants which do specifically name or describe every person, organisation or set of premises individually, modifications must be made to add, vary or remove any names or descriptions.

5.23 Where a thematic warrant does not individually name or describe additional persons, organisations or sets of premises, but either describes the thematic subject-matter alone, or provides descriptions within the subject matter (for example 'a group of persons carrying out a particular crime') modifications are not required to intercept, or obtain secondary data from, the communications of any additional person, organisation or set of premises as long as one of these conditions is met.

a) Where it has not been reasonably practicable to provide any additional details, the person, organisation or set of premises fall within the thematic subject-matter; or

b) Where it has been reasonably practicable to provide details in the form of general descriptions falling within the subject matter, the persons, organisations or sets of premises fall within one of those general descriptions.

5.24 Modifications to add individual names or descriptions are not necessary in these circumstances as the warrant already provides lawful authority to intercept, or obtain secondary data from, the communications falling within the subject matter or within any of the descriptions of those persons, organisations or sets of premises that may have been provided. As described in paragraphs 5.18 and 5.19, the Secretary of State must consider the authorised conduct to be necessary and proportionate before issuing the warrant and must clearly understand the extent of the conduct that they are authorising.

5.25 In accordance with section 34(6) an intercepting agency is permitted to amend a warrant (including the name or description included in relation to the subject-matter)as long as such an amendment does not alter the conduct that is authorised by the warrant. An example of this would be to correct the spelling of a person's name.

5.26 If, over the course of an operation, an intercepting agency considers that the nature of the operation has developed in such a way that the authorised activity might not be considered necessary and/or proportionate, they must consider whether the warrant should be modified pursuant to the requirement to ensure that any warrant remains necessary and proportionate. If the agency determines the warrant is no longer necessary and proportionate, even if modified, then it must be cancelled.

5.27 There is an on-going duty to review warrants and to cancel them if they are no longer considered to be necessary and proportionate. More detail regarding the cancellation of warrants can be found in paragraphs 5.92 and 5.93.

Example: *An intercepting agency may seek a warrant to intercept the communications of persons who are understood to be resident in a shared house and they will need to be rapidly investigated. The agency sets out in the application that they will be unable to individually name or describe the residents in advance due to the speed of the work. However, over the course of the operation, the agency determines that only a proportion of people falling within the description of 'residents at C' are of intelligence interest. The intercepting agency must assess whether the necessity and proportionality case put to and accepted by the Secretary of State and Judicial Commissioner remains accurate or needs to be narrowed. If the change in circumstances affects the necessity or proportionality of the warrant activity then the warrant may need to be modified to reflect more precisely those subject to interference or the Secretary of State should be notified that the warrant may need to be cancelled.*

Renewal of thematic warrants

5.28 The provisions relating to renewal of warrants, described further in paragraph 5.62, apply to thematic warrants. An agency seeking to renew a thematic warrant must present in the renewal application a thorough assessment of the proportionality of conduct to date, including any collateral intrusion, and the extent of any interference with privacy. In particular, when seeking to renew a thematic warrant that does not specifically name or describe each person, organisation or set of premises the applicant should explain how the warrant continues to meet the requirements of section 31. The renewal application should provide any further, relevant information about those who fall within the subject-matter of the warrant and, if relevant the additional details provided in order to sufficiently enable the proper assessment of the proportionality and intrusion involved in the interception.. This information will ensure that the Secretary of State and Judicial Commissioner will have further opportunity to consider the necessity and proportionality of the interference, supported by up to date information.

5.29 The following examples provide an illustration of operational scenarios in which the use of a thematic interception warrant would be appropriate.

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 Agency conducts operations to understand weapons systems, gaining intelligence that gives insight into the capability, deployment and use of weapons systems. One example of this is naval vessels, where the main purpose is to obtain intelligence about the movements and capabilities of those vessels, and not the personal data of individuals. A warrant is sought to intercept, or obtain secondary data from, communications associated with vessels controlled or operated by state organisations posing a threat to the UK. When UK military aircraft deploy, the threat needs to be understood to protect the aircrew. Signals – such as those related to potentially hostile air defence forces – are intercepted by relying on a warrant for interception of communications of weapons systems owned, controlled or operated by relevant state organisations. These warrants mean that the Agency can intercept data from weapons systems wherever they are in the world and UK military equipment can be developed and used effectively to defend against threats.

Format of warrant application

Targeted interception warrants

5.30 In this chapter, reference to an ‘application’ for a warrant includes the application form and the draft warrant (including the draft instrument and any draft schedules). An application for a targeted interception warrant, a copy of which must be retained by the applicant should contain the following information:

a) The statutory ground(s) for which the warrant being issued is considered necessary. Any application for a warrant for the purpose of safeguarding the economic well-being of the UK should identify the circumstances that are relevant to the interests of national security.

b) The background to the operation or investigation in the context of which the warrant is sought and what the operation or investigation is expected to deliver;

c) An application 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.

d) An application 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.

e) 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.

f) An application 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.

g) A description of the communications to be intercepted or the secondary data to be obtained, details of the communications service provider(s), an assessment of the feasibility of the interception to the extent known at the time of the application and an outline of how obtaining the material will benefit the investigation or operation;[5]

h) A description of the conduct to be authorised or the conduct it is expected will be 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

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, whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means;

j) Where a thematic warrant either lists the subject-matter alone, or provides additional details by means of general descriptions rather than individual names or descriptions, the warrant application should say why it is not reasonably practicable to individually name or describe persons, organisations or sets of premises;

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

l) Whether the warrant is likely or intended to result in the obtaining of legally privileged material, a statement to that effect, an assessment of how likely it is that such material will be included and what protections it is proposed will be applied to the handling of information so obtained;

[5] 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 (for example the International Mobile Subscriber Number (IMSI). Such a number or address may be temporary or permanent.

m) Where the purpose, or one of the purposes, of the warrant is to intercept items subject to legal privilege, a statement to that effect and an assessment of why there are exceptional and compelling circumstances that make the interception of such items necessary and what protections it is proposed will be applied to the handling of the information so obtained;

n) If the intention is to obtain items that would be subject to legal privilege if the communications were not made with the intention of furthering a criminal purpose, the application should contain a statement to that effect and set out the reasons for believing that the communications will be made with the intention to further a criminal purpose.

o) Where the purpose of the warrant is to obtain communications of a member of a relevant legislature (as defined in section 26) (see Chapter 9), a statement to that effect and what protections it is proposed will be applied to the handling of the information so obtained;

p) Where the warrant is intended to authorise or require obtaining communications or other items of information which the applicant believes will contain confidential journalistic material or to identify or confirm the source of journalistic information or obtain confidential journalistic information, a statement to that effect and what protections it is proposed will be applied to the handling of the information so obtained;

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

r) 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).

5.31 When completing a warrant application, the intercepting agency must ensure that the case for the warrant is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which support or weakens the case for the warrant.

Targeted examination warrants

5.32 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 152(4) of the Act, of intercepted content obtained under a bulk interception warrant of an individual known at that time to be in the British Islands.

5.33 Targeted examination warrants must be issued by the Secretary of State or, where relevant, the Scottish Ministers, 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 and what the operation or investigation is expected to deliver;

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;[6]

c) Where a warrant relates to a group of persons 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 persons 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) Where a warrant that relates to any testing, maintenance, development and/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;

f) A description of the relevant content that is to be selected for examination[7];

g) An explanation of why the selection for examination is considered to be necessary on one or more of the grounds set out in section 20(2) or 21(4). Any application for a warrant for the purpose of safeguarding the economic well-being of the UK should identify the circumstances that are relevant to the interests of national security.;

h) Consideration of why the selection for examination to be authorised by the warrant is proportionate to what is sought to be achieved, including whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means;

i) Where a thematic warrant either lists the subject-matter alone, or provides additional details by means of general descriptions rather than individual names or descriptions, the warrant application should say why it is not reasonably practicable to individually name or describe persons, organisations or sets of premises;

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

k)

l) Where the purpose, or one of the purposes, of the warrant is to examine items subject to legal privilege, a statement to that effect and an assessment of why there are exceptional and compelling circumstances that make the examination

[6] Reference to naming or describing for c), d) and e) of the list (which relate to thematic warrants), may be done in draft schedules which form part of the application. The submission must include information regarding how and when naming of individuals will be achieved on an ongoing basis.

[7] 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 communications service provider (for example the International Mobile Subscriber Number (IMSI). Such a number or address may be temporary or permanent.

of such items necessary and that protections it is proposed will be applied to the handling of the information so obtained;

m) Where is is considered likely that legally privileged items will be included in the communications to be examined, a statement to that effect and an assessment of how likely it is that such items will be included in the communications and what protections it is proposed will be applied to the handling of information so obtained;

n) If the intention is to select for examination items that would be subject to legal privilege if the communications were not made with the intention of furthering a criminal purpose, the application should set out the reasons for believing that the communications will be made with the intention to further a criminal purpose;

o) If the intention is to select for examination items that would be subject to legal privilege if the communications were not made with the intention of furthering a criminal purpose, the application should set out the reasons for believing that the communications were made with the intention to further a criminal purpose;

p) Whether the purpose of the warrant is to examine communications of member of a relevant legislature (as defined in section 26) (see Chapter 9), and if so what protections it is proposed will be applied to the handling of the information so obtained;

q) Where the warrant is intended to authorise the selection for examination of material which the application believes is confidential journalistic material or to identify or confirm the source of journalistic information a statement to that effect and what protections it is proposed will be applied to the handling of the information so obtained;

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

s) 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

5.34 In addition to the information at paragraph 5.32 above which apply equally to mutual assistance warrants, section 40(3) 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

Format of targeted warrants

Targeted interception warrants

5.35 Each new warrant will typically comprise three sections:

- a warrant instrument signed by the Secretary of State describing the subject-matter of the warrant,
- a schedule of identifiers to be used for identifying the communications to be intercepted which each communications service provider will receive as appropriate, and
- a schedule(s) that names or describes the persons, organisations or sets of premises as far as reasonably practicable.

5.36 Only the warrant instrument and 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,(for example, because of uncertainty over real identity) descriptions on the instrument can be in the form of an alias or other description that identifies the person, organisation or set of premises.

5.37 The warrant 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 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;
- A warrant that relates to any testing, training activities, maintenance or the development of capabilities must describe the nature of the testing, training, maintenance or development of those capabilities;
- Date the warrant was issued.
- 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.[8] The warrant must specify (or describe[9]) 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 as far as possible;

Targeted examination warrants

5.38 Each warrant will comprise a warrant instrument signed by the Secretary of State and may also include a schedule or set of schedules describing the subject matter of the warrant.

- The warrant will include A statement that it is a targeted examination 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 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.
- A warrant that relates to any testing or training activities must describe those activities
- Date the warrant was issued.

- A warrant reference number; and

[8] 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 communications service provider (for example the International Mobile Subscriber Number (IMSI). Such a number or address may be temporary or permanent.

[9] See section 263(1) of the Act.

- A means of identifying the communications content that is to be selected for examination.[10] The warrant must specify (or describe[11] 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 as far as possible.

Mutual assistance warrants

5.39 Each mutual assistance warrant will include:

- A statement that it is a mutual assistance warrant;
- The person to whom 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 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

5.40 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:

[10] 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 Communications Service Provider. Such a number or address may be temporary or permanent.

[11] See section 263 of the Act.

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

5.41 The Secretary of State or, where appropriate, the Scottish Ministers may only issue a warrant under section 19 if they consider the following tests are met:

- The warrant is necessary:[12]

  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 may 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.

- 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 less intrusive 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 received approval from the Prime Minister where the additional protection for Members of Parliament and other relevant legislatures applies (see section 26 of the Act).

- The Secretary of State is satisfied that there are exceptional and compelling circumstances where the purpose, or one of the purposes, of the warrant is to intercept or select for examination items subject to legal privilege.

- The Secretary of State is satisfied that specific arrangements are in place for the handling, retention, use and destruction of items subject to legal privilege where the warrant is likely to result in the interception or selection for examination of such items.

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

- Where the purpose, or one of the purposes, of the warrant is to intercept or select for examination communications containing confidential journalistic information or to identify or confirm a source of journalistic information, the Secretary of State is satisfied that specific arrangements are in place for the handling, retention, use and destruction of such communications.

- The Secretary of State has complied with Section 2 of the Act, which imposes general duties in relation to privacy. The Secretary of State must consider: whether what is sought to be achieved by the warrant could be achieved by less intrusive means; whether the level of protection to be applied to information obtained under the warrant is higher because of the particular sensitivity of that information; the public interest in the integrity and security of telecommunications systems and postal services; and any other aspects in the public interest in the protection of privacy.

- 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.

5.42 Section 40 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

5.43 Part 2 warrants may be issued by the Scottish Ministers for the purpose of the prevention and detection of serious crime or, in the case of a mutual assistance warrant, for the purpose of giving effect to an EU mutual assistance warrant or an international mutual assistance warrant. In this code references to the "Secretary of State" should be read as including the Scottish Ministers where appropriate. The functions of the Scottish Ministers cover renewal, modification and cancellation arrangements. Sections 21 and 22 of the Act make provision for the Scottish Ministers to issue targeted interception warrants for serious crime purposes in certain circumstances. The Scottish Ministers may issue a targeted interception warrant or a targeted examination warrant if the warrant, if issued, would relate to a person, group of persons or set of premises in Scotland, or reasonabl believed to be in Scotland, at the time the warrant is issued. They may also issue a mutual assistance warrant if it would relate to a person or group of persons, or to premises in Scotland.

5.44 The 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 warrant: senior official signature

5.45 The Act permits that when it is not reasonably practicable for the Secretary of State or member of the Scottish Government to sign a Part 2 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 their constituency. The Secretary of State or member of the Scottish Government must still personally authorise the conduct authorised by the warrant. When seeking authorisation the senior official must explain the case, either in writing or orally, to the Secretary of State or member of the Scottish Government and this explanation should cover the considerations and information that would be included on an application form as set out at paragraph 5.8. This will include an explanation of necessity and proportionality. Once authorisation has been granted the warrant may be signed by a senior official. If the Secretary of State or member of the Scottish Government 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.

Consideration of collateral intrusion

5.45 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, targeted examination warrant, or mutual assistance warrant should state whether the interception or selection for examination is likely to give rise to a degree of collateral intrusion 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, targeted examination warrant or mutual assistance 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 or, in the case of thematic warrants, modifying the warrant to add those individuals if permissible.

Judicial commissioner approval

5.46 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. The Judicial Commissioner will review the warrant issuer's conclusion as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. In reviewing these conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. The Judicial Commissioner must review the conclusions 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).

5.47 The Judicial Commissioner may seek clarification from the warrant granting department or warrant seeking agency as part of those considerations.

5.48 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). An urgent warrant which is not approved by a judicial commissioner cannot be appealed to the IPC.

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

5.50 Where a Judicial Commissioner refuses the decision to issue the warrant, they must provide written reasons for doing so

Urgent authorisation of a targeted interception warrant

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

5.52 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 one or both of the following 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 or 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.

5.53 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.

5.54 If the Judicial Commissioner approves 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 warrants. Where the Secretary of State decides to renew an urgent warrant prior to its approval by a Judicial Commissioner, the original decision to issue the urgent warrant may be considered by the Judicial Commissioner at the same time as they are considering the Secretary of State's decision to renew the warrant.

5.55 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.

5.56 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 individual 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, and so at that point an interception warrant was not sought. More information comes to light and it is now suspected that they are an agent of the hostile nation and 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 targeted warrants

5.57 A targeted interception warrant, targeted examination warrant or mutual assistance warrant issued using the non-urgent 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.

5.58 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[13]. 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[14].

5.59 Where a combined interception warrant includes warrants or authorisations which would cease to have effect at the end of different periods, the combined warrant will expire at the end of the shortest of those periods.

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

5.61 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 notify the Secretary of State.

Renewal of targeted interception/ examination warrants

5.62 Section 31 of the Act sets out that the Secretary of State may renew a warrant at any time during the renewal period. The renewal period is 30 days before the warrant would otherwise cease to have effect. 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.

5.63 Sections 26 (Members of Parliament etc), 27 (items subject to legal professional privilege) 28 (confidential journalistic material) and 29 (sources of journalistic material) apply in relation to the renewal of warrants in the same way as they apply to a decision to issue a warrant. Where confidential or privileged material has been obtained during an investigation or operation and is being retained other than for the purpose of destruction, this information should be included in the application for the renewal of the warrant

5.64 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 for one or more operational purposes in breach of the prohibition in section 152(4) of the Act on seeking to identify communications of individuals in the British Islands.

5.65 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 5.38.

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

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

5.66 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.

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

5.68 In those circumstances where the assistance of communications service providers has been sought, a copy of the warrant renewal instrument (or part of that instrument that is relevant to the particular Communications Service Provider or other person) 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.

Modification of targeted warrants

5.69 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 initially to consider whether the modification being sought is minor or major. 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.

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

Major Modifications

5.71 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 permissible. A major modification of this type cannot be made to a warrant which relates to a 17(1) targeted “non-thematic” warrant i.e. where the warrant relates to a particular person, organisation or a single set of premises. Whether or not a thematic warrant will be subject to the major modification process will depend on the particular circumstances of the case and how the subjects of that warrant are described. Further detail on the circumstances in which major modifications apply to thematic warrants are included at paragraphs 5.34 to 5.38. 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[15]:

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

- 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[16] acting on behalf of the Secretary of State or (as the case may be) the Scottish Ministers.

5.72 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 (Members of Parliament and other relevant legislature), 27 (Items subject to legal privilege) or 28 and 29 (confidential journalistic material or sources of journalistic information) apply (further information is provided in Chapter 9).

5.73 In practice, this means that major modifications may be made where permissible to a targeted thematic warrant to add or vary the name or description of a person, organisation or set of premises to which the warrant relates. 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 a person, organisation or set of premises. In practice this means that a warrant which relates to a particular person, premises or organisation 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 subject matter of the original warrant.

5.74 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. X'. The Secretary of State, with Judicial Commissioner approval, issues the warrant authorising the interception of Mr. X's communications. The investigation progresses and the intercepting agency wants to intercept the communications of one of Mr. X's associates. This would require a new warrant – the warrant against Mr. X cannot be modified so as to be against an additional person.

Example of a modification that WOULD be permitted:
An intercepting agency obtains a targeted thematic interception warrant as part of a single investigation relating to a serious criminal known as 'Mr. X' and his associates 'Mr Y' and 'Mr Z'. The Secretary of State, with Judicial Commissioner approval, issues the warrant authorising the interception of Mr. X and his associates investigated under Operation "NAME". The investigation progresses and the intercepting agency wants to intercept another one of Mr. X's associates 'Miss A'. The warrant could be modified to add the associate, and the factors to be used to identify her communications. This would require a major and minor modification (see further below)).

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

Minor modifications

5.75 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.

5.76 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 applied for 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[17] 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 grade in the same intercepting agency as the person to whom the warrant is addressed.

5.77 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[18] 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.

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

[18] 34(10)

Urgent major modification of targeted warrants

5.78 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 the intercepting agency has received intelligence that a quantity of drugs is imminently going to enter the country.

5.79 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 three 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.

Warrant cancellation

5.80 Any of the persons authorised to issue warrants under Part 2 may cancel a warrant at any time. In addition, a senior official acting on behalf of the Secretary of State may cancel a warrant issued by the Secretary of State[19]. 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.

5.81 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 everyone on whom the warrant was served since it was issued or last renewed.

[19] A Senior Official acting on behalf of the Scottish Ministers may cancel a warrant issued by the Scottish Ministers.

Combined warrants

5.84 Schedule 8 to the Act provides for combined warrants. Combining warrant applications is not mandatory, but provides the option for grouping warrants and authorisations 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 reduces duplication of identical information across warrant applications. Any application for a combined warrant or authorisation must include a statement that it is a combined application and must set out the warrants and authorisations it includes.

5.85 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 conduct required for an operation was authorised by a combined equipment interference and interception warrant and the interception was no longer necessary and proportionate, 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 equipment interference that remains necessary and proportionate. Combined warrants may also be applied for on an urgent basis.

5.86 Where warrants of different durations are combined, the shortest duration applies, 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.

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

5.88 The duties imposed by section 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 section 2.

5.89 The Act provides that it is possible only to serve the part of a combined warrant that is an interception warrant. For example, if a combined warrant included a targeted interception warrant and an authorisation for another investigatory power that did not require the assistance of another person, such as a telecommunications operator, to provide assistance in giving effect to it, it is possible to serve the targeted interception warrant, without serving the other authorisation.

5.90 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, section 41(duty of operators to assist with implementation) would apply to the targeted interception part of a combined warrant but only to that part.

5.91 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. Section 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.

5.92 The exclusion of matters from legal proceedings (section 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 reveals the existence of an interception warrant, the material is excluded from use in legal proceedings according to section 53 of the Act.

5.93 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

5.94 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 warrant under section 5 of the Intelligence Services Act 1994

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

5.96 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 warrants. However, where a warrant under section 5 of the Intelligence Services Act forms part 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

5.97 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

5.98 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 106
- 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

5.99 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 RIP(S)A (or in certain circumstances 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 RIP(S)A.

5.100 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.

5.101 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.

5.102 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 warrant under section 5 of the Intelligence Services Act 1994

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

If a law enforcement agency wished to conduct an operation which involves directed surveillance (provided for under Part 2 of RIPA) and targeted interception, they may wish to combine these applications, 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.)

6. Bulk interception warrants

6.1 This chapter 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 may only be issued to the security and intelligence agencies and 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 136 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 do one or more of the following: to intercept communications described in the warrant, to obtain secondary data from such communications, to select for examination the intercepted content or secondary data, or the disclosure of anything obtained under 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 both the interception of communications and/or the obtaining of secondary data from such communications in the course of their transmission and the selection for examination of particular communications content or secondary data obtained under the warrant. In practice, several different processing systems may be used to effect the interception and/or the obtaining of secondary data, and the selection for examination of the data so obtained.

6.5 These processing systems process data from the communications links or signals that the intercepting agency has chosen to intercept. A degree of filtering is then applied to the traffic on those links and signals, designed to select types of communications of potential intelligence value whilst discarding those least likely to be of intelligence value. As a result of this filtering, which will vary between processing systems, a significant proportion of the communications on these links and signals will be automatically discarded. Further complex searches may then take place to draw out further communications most likely to be of greatest intelligence value, which relate to the agency's statutory functions. These communications may then be selected for examination for one or more of the operational purposes specified on the warrant where the conditions of necessity and proportionality are met. Only items which have not been filtered out can potentially be selected for examination by authorised persons.[20]

6.6 A bulk interception warrant will usually be served on a communications service provider to provide assistance with giving effect to it. This may, for example, 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.

6.7 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 a strategic intelligence gathering capability, whereas targeted interception is primarily an investigative tool that is used once a particular subject for interception has been identified.

6.8 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 136(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.

[20] Authorised persons is used in this Code to mean an officer who has a suitable level of training and security clearance and who is permitted to select bulk data for examination.

6.9 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.

6.10 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 136 and 137 of the Act describe what constitutes secondary data in the context of bulk interception. Secondary data comprises systems data (see section 264(4)) and identifying data (see section 264(2)) that is comprised in or associated with the communication. Systems data is any data that enables or facilitates system or service function. Identifying data is data which may be used to identify, or assist in identifying, any person, apparatus, system, service, event or location (secondary data is explained further in Chapter 2).

6.11 The Act therefore enables an intelligence service 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.

6.12 Section 136(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.

6.13 Section 142(3) 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 highly likely that a bulk interception warrant will specify the full range of operational purposes as set out at section 142(5), and which is explained in more detail in the “Examination Safeguards” section of this chapter.

6.14 When an authorised person within the intercepting agency selects communications for examination, documentation must exist that provides an explanation of why it is necessary for one or more of the operational purposes specified on the warrant, and why it is proportionate. 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).

Format of warrant applications

6.16 An application for a bulk interception warrant is made to the Secretary of State. As set out at section 138 of the Act, bulk interception warrants are only available to the intelligence agencies. In this chapter, reference to an 'application' for a warrant includes the application form and the draft warrant (including the draft instrument and any draft schedules). 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). A bulk warrant must always be necessary in the interests of national security. The scrutiny of the application will 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 each of the operational purposes specified.

6.19 Each application, a copy of which must be retained by the applicant, should contain the following information:

a) Background to the application;

b) 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;[21] and

c) 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

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

out at section 136(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.

d) The operational purposes for which the content and secondary data may be selected for examination and an explanation of why examination is or may be necessary for those operational purposes proposed in the warrant;

e) Consideration of whether intercepted content or secondary data obtained under the warrant may be made available to any other security and intelligence agency or an international partner, where it is necessary and proportionate to do so.

f) 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;

g) 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 what is sought to be achieved could not reasonably be achieved by less intrusive means;

h) 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 152 of the Act; and

i) 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 150 of the Act.

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 giving effect to the warrant. Communications service providers are unlikely to receive a copy of the operational purposes specified in the warrant. The warrant should include the following:

a) The fact that it is a Bulk Interception Warrant;

b) A description of the communications to be intercepted and/or from which secondary data will be obtained;

c) The operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination;

d) Date the warrant was issued; and

e) The warrant reference number.

Authorisation of a bulk interception warrant

6.21 A bulk interception warrant may only be issued if the Secretary of State considers that the main purpose of the warrant is to intercept overseas-related communications, and/or obtain secondary data from those communications.

Necessity

6.22 Before a bulk interception warrant can be issued, the Secretary of State must consider that the warrant is necessary for one or more of the statutory purposes, as at 138(1)(b) and (2). One of these statutory purposes must always be national security. If the Secretary of State is not satisfied that the warrant is necessary in the interests of national security, then it cannot be issued.

6.23 Before a bulk interception warrant can be issued, the Secretary of State 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 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 138(1)(b) and (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, the selection for examination for each specified operational purpose on that warrant must be necessary for one or both of these two broader purposes. In cases where it is necessary and proportionate for content or secondary data obtained under the warrant to be made available to another of the security and intelligence agencies or an international partner, the operational purposes specified in the warrant may include operational purposes relating to that third party providing the tests in section 138(1)(d) are met.

6.24 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 138(1)(b) or section 138(2) purpose, and which meets the conditions set out in section 152 is, in fact, selected for examination. The Investigatory Powers Commissioner is under a duty to review the adequacy of those arrangements.

Proportionality

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

6.26 In considering whether a bulk interception warrant is necessary and proportionate, the Secretary of State 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

6.27 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

6.28 Before a bulk interception warrant can be issued, the Secretary of State's decision to issue it must be approved by a Judicial Commissioner. Section 140 of the Act sets out the test that a Judicial Commissioner must apply when considering whether to approve the decision. The Judicial Commissioner will review the Secretary of State's conclusion as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. The Judicial Commissioner will also review the Secretary of State's conclusions as to whether each of the operational purposes specified on the warrant is a purpose for which selection is, or may be, necessary. And the Judicial Commissioner will also, where relevant, review matters the Secretary of State has taken into account in circumstances where there are additional requirements in respect of warrants affecting overseas operators, in accordance with section 139 of the Act.

6.29 In reviewing these conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. The Judicial Commissioner must when carrying out the Judicial Commissioner's review comply with the duties imposed by section 2 (general duties in relation to privacy).

6.30 The Judicial Commissioner may seek clarification from the warrant granting department or warrant seeking agency as part of their considerations.

6.31 If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either:

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

6.32 If the IPC refuses the decision to issue a warrant the Secretary of State must not issue the warrant. There is no further avenue of appeal available in the Act.

6.33 Where a Judicial Commissioner refuses the decision to issue the warrant, they must provide written reasons for doing so.

Additional requirements in respect of warrants affecting overseas operators

6.34 As set out at section 139, 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.

6.35 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.

6.36 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 139(3), 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.

6.37 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.

Duration of bulk interception warrants

6.38 Bulk interception warrants are valid for an initial period of six months. Upon renewal, warrants are valid for a further period of six months. Where modifications are made to a bulk interception warrant, the warrant expiry date remains unchanged.

Renewal of a bulk interception warrant

6.39 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 144 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.

6.40 In deciding to renew a bulk interception warrant, the Secretary of State 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).

6.41 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.

6.42 Where the Secretary of State is 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.

6.43 In those circumstances where the assistance of communications service providers has been sought, a copy of the warrant renewal instrument (or part of that warrant that is relevant to the particular Communications Service Provider or other person) 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.

Modification of a bulk interception warrant

6.44 A bulk interception warrant may be modified at any time by an instrument issued by the person permitted to do so by section 145 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 to the communications described in the 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 145 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.

6.45 In circumstances where a modification is being made to add or vary an operational purpose, this is a **major modification** and it must be made by a Secretary of State and must be approved by a Judicial Commissioner before the modification comes into force. The Act permits that when it is not reasonably practicable for the Secretary of State to sign a major modification instrument a delegate may sign it 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 their constituency. The Secretary of State must still personally authorise the modification.

6.46 Once the modification has come into force, the added or varied operational purpose may be used to select for examination any content or secondary data obtained under the warrant, even if this material was intercepted or obtained prior to the addition or variation of the operational purpose.

6.47 In circumstances where a bulk interception warrant is being modified to remove an operational purpose, this is a **minor modification** and 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 must modify the warrant to remove that operational purpose

6.48 As set out at paragraphs 6.4-6.15 a bulk interception warrant may authorise the interception of communications and/or the obtaining of secondary data and 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 interception or obtaining of secondary data, 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 of data already obtained under the warrant.

6.49 Such a modification is a **minor modification** and 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.

6.50 In accordance with section 145(13) an intercepting agency is permitted to amend a warrant (including the name or description included in relation to the subject-matter)as long as such an amendment does not alter the conduct that is authorised by the warrant. An example of this would be to correct a spelling.

Urgent modifications of a bulk interception warrant

6.51 In urgent cases a major modification adding or varying an operational purpose can be made by a Secretary of State. An example of 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.

6.52 Where a major modification is made in an urgent case, a statement of that fact must be included on the modifying instrument, and the modification must be approved within three working days following the date of issue by a Judicial Commissioner. If a Judicial Commissioner refuses to approve the modification, the modification will cease to have effect. That refusal does not affect the lawfulness of anything done between the modification being made and the Judicial Commissioner reviewing and refusing the modification.

6.53 Where a Judicial Commissioner refuses to approve the urgent modification, the Secretary of State may not refer the case to the Investigatory Powers Commissioner.

Warrant cancellation

6.54 The Secretary of State, or a senior official acting on their behalf, may cancel a bulk interception warrant at any time. Such a person 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 138(1)(b) or 138(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.

6.55 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.

6.56 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 existing communications service providers, if any, who have given effect to the warrant during the preceding twelve months.

6.57 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.

Examination safeguards

6.58 Section 152 of the Act provides specific safeguards relating to the selection for examination of intercepted content and secondary data acquired through a bulk interception warrant. Further guidance on these safeguards is provided below.

6.59 Sections 152(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 142 of the Act. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination. 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.

6.60 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 142 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.

6.61 Section 142 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

6.62 Section 138 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 142 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.

6.63 Section 145 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 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 142 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 Act 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.

6.64 In addition to the central list of operational purposes having to be approved by the Secretary of State, section 142 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.

6.65 Although bulk interception warrants are authorised for the purpose of acquiring overseas-related communications, section 136(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 152 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).[22]

6.66 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.

[22] 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

6.67 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.

6.68 The analysis of bulk systems data and identifying data (referred to here as secondary data) is the primary means by which the security and intelligence agencies are able to discover and assess threats to the UK. This can only be achieved effectively through the aggregation of non-content data from a wide range of sources acquired under multiple bulk warrants, not limited to bulk interception warrants. Such analysis allows the agencies to draw together fragments of information into coherent patterns, which allow for the identification of those threats while at the same time minimising intrusion into privacy.

6.69 The analysis of aggregated bulk secondary data is also essential to the understanding of how communications are routed over the internet at any given time. Secondary data analysis is therefore crucial to enable the optimisation of interception of the content of communications, as well as the obtaining of secondary data itself.

6.70 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.

6.71 No data may be selected for examination other than in accordance with the specified operational purposes. In general, automated systems should, where technically possible, be used to effect the selection for examination in accordance with section 142 of the Act. A limited number of officials may also be permitted to access the system during the processes of filtering, processing and selection for examination, for example to check system health. Such access must itself be necessary on the grounds specified in sections 129(1)(b) and 129(2) and where such access involves selection for examination of content or secondary data it must be necessary for an operational purpose specific on the warrant. Agency arrangements for such access will be kept under review by the Investigatory Powers Commissioner during his or her inspections..

6.72 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 152 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 security cleared.

6.73 No content or data may be selected for examination for the specified operational purposes unless this is necessary and proportionate in all the circumstances. In addition, arrangements must be put in place to provide for the creation and retention of documentation (for the purposes of subsequent examination or audit) outlining why access to the content or data by authorised persons is necessary and proportionate and the applicable operational purposes. Systems should, to the extent possible, prevent access to the content or data unless such documentation has been created. The documentation must also record the reasons why any collateral intrusion into privacy is considered proportionate and any steps to minimise it. All documentation must be retained in accordance with agreed policy for the purposes of subsequent examination or audit.

6.74 Authorised persons may be granted access to systems containing intercepted content or secondary data only for defined periods of time, after appropriate training, and where it is necessary for them to have access. Access may be renewed where these conditions continue to be met.

6.75 Periodic audits should be carried out to ensure that the requirements set out in section 152 of the Act are being met. These audits must include checks to ensure that the documentation justifying 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.

6.76 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.

6.77 The Prime Minister must approve any application to select for examination the communications of a member of a relevant legislature obtained under a bulk interception warrant.

Selection for examination of intercepted content in breach of the section 152(4) prohibition

6.78 Any selection for examination of the content of the communications intercepted must also meet the selection conditions set out at section 152(3). Section 152(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 152(5).

6.79 Selection for examination in breach of the prohibition in section 152(4) of the Act may be authorised by section 152(5). Section 152(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 to the UK. To enable the selection for examination to continue, sections 152(5) and 152(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 152(5) the Secretary of State must be notified.

Offence of breaching examination safeguards

6.80 Any intercepted content or secondary data obtained under a bulk interception warrant may only be selected for examination subject to the safeguards in sections 152 and 153 of the Act. Section 155 of the Act makes it an offence for a person deliberately to select such content or data for examination in breach of these safeguards where that person knows or believes such selection does not comply with the safeguards.

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 41 of the Act then allows the intercepting agency to carry out the interception, and/or to require the assistance of other persons in giving effect to the warrant. Section 41 makes clear that the warrant may be served on any person, inside or outside the UK, who may be able to provide such assistance in relation to that warrant. The same process applies for bulk interception warrants and is set out at section 149 of the Act.[23]

7.3 Where a copy of an interception warrant or mutual assistance warrant has been served on anyone providing a postal service or offering or providing a telecommunications service, to a person in the UK, or who has control of, or provides a telecommunications system which is wholly or partly in the UK, that person is under a duty to take all such steps for giving effect to the warrant as are notified to the person by or on behalf of the intercepting authority. This applies to any company offering or providing services to persons in the UK, irrespective of where the company is based. Section 43 sets out the means by which that duty may be enforced.

7.4 Section 42 of the Act provides that service of a copy of a targeted interception warrant or mutual assistance 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 149 of the Act makes clear that sections 42 and 43 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, or any other means, are reasonably practicable). The intercepting agency must take steps to bring the contents of the warrant to the attention of the relevant person.

[23] [23] Section 139 imposes additional requirements in respect of warrant affecting overseas providers.

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 or mutual assistance 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 43 and section 149). The steps which may be required of communications service providers are limited to those which it is reasonably practicable to take (section 43(4)). The duty to comply with a warrant applies only to a person who is capable of complying with it. Where a technical capability notice is in place and consideration is being given to a provider's compliance with the duty, the steps which it is reasonably practicable for the provider to take will include every step which it would have been reasonably practicable for the provider to take if the provider had complied with all of the obligations in the notice. Knowingly failing to comply is an offence which, on summary conviction in the UK, may result in imprisonment and/or a fine.

7.6 When considering whether it is reasonably practicable for a communications service provider outside the UK to take any steps in a country or territory outside the UK, regard must be given to any requirements or restrictions under the law of that country or that are relevant to the taking of those steps. The communications service provider should work with the Government to find ways for the provider to comply in a manner 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, no conflict of laws issues will prevent the communications service provider from complying 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 must be considered by the Secretary of State on a case-by-case basis, taking into account the individual circumstances of the relevant communications service provider.

7.9 Section 139 details the additional requirements that apply 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. These requirements are detailed at paragraphs 6.32-6.35 above.

7.10 A copy of the warrant must be served in such a way as to bring the contents of the warrant to the attention of the person or communications service provider who the intercepting agency considers can provide assistance in relation to it. The agency may provide the following to the person or 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 the warrant specifying this information 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 are unlikely to 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 to notify the communications service provider of steps they are required to take to give effect to the warrant[24] 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) but will not necessarily be provided with all the information contained in the warrant.

7.11 Section 237 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 249 of the Act recognises that communications service providers incur costs in complying with requirements in the Act, including the interception of communications in response to requests under Part 2 and Chapter 1 of Part 6 of the Act. The Act, therefore, requires the Secretary of State to have in place arrangements to ensure that operators receive an appropriate contribution to these costs.

[24] See section 43(1).

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 serious crime or are involved in acts of terrorism. The provision of public funding may be subject to terms and conditions determined by the Secretary of State.

7.15 It is legitimate for a communications service provider to seek contributions towards its costs which may include an element of funding towards 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, certain staff benefits or arrangements made in line with the terms and conditions of employment, such as bonuses paid to members of staff that are reflective or representative of the company's performance, will be excluded from this category of costs. Such matters are arranged between the employer and employee and the Government does not accept responsibility for such costs. Further details with respect to cost recovery will be available in the handbook provided to all communications service providers who maintain an interception capability.

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 Secretary of State such information as the Secretary of State 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 253 of the Act to provide a technical capability to give effect to interception, equipment interference and bulk acquisition warrants and notices or authorisations for the acquisition of communications data. The purpose of maintaining a technical capability is to ensure that, when a warrant, authorisation or notice 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. The Secretary of State may only give a notice where the decision to do so has been approved by a Judicial Commissioner. In practice, technical capability notices will only be given to communications service providers that are likely to be required to give effect to warrants, authorisations or notices given under Part 3 of the Act on a recurrent basis.

8.3 The only obligations that may be imposed by a technical capability notice are those set out in regulations made by the Secretary of State and approved by Parliament. Section 253(4) limits the obligations that the Secretary of State may include in those regulations.

8.4 Section 253(5) gives examples of the sorts of obligations that such regulations may include:

- 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.

8.5 . An obligation can only be imposed by a technical capability notice for the purpose of securing that it is (and remains) practicable to impose requirements on a communications service provider, and that the provider is capable of providing the necessary technical assistance to meet these requirements. For example, an obligation relating to the security of a telecommunications service or system can be imposed by a technical capability notice for the purpose of ensuring that the operator has the capability to provide assistance in relation to an interception warrant.

8.6 An obligation imposed by a technical capability notice on a communications service provider to remove encryption does not require the provider to remove encryption per se. Rather, it requires that provider to maintain the capability to remove encryption when subsequently served with a warrant, notice or authorisation. Such an obligation may only relate to electronic protections that the company has itself applied to communications or data, or where those protections have been applied on behalf of that communications service provider, and not to encryption applied by any other party. 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.

8.7 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 is able 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 capability, particularly if more than one communications service provider applies electronic protections to communications and data.

8.8 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, a warrant may require a communications service provider to take such steps as are reasonably practicable to take to give effect to it. This will include, where applicable, providing communications or data in an intelligible form. An example of such circumstances might be where a communications service provider removes encryption from communications or data for their own business reasons.

Consultation with service providers

8.9 Before giving a notice, the Secretary of State must consult the communications service provider.[25] In practice, informal consultation is likely to take place long before a notice is given. The Government will engage at the outset 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.

8.10 In the event that the giving of a notice to a communications service provider is deemed appropriate, the Secretary of State must consult the communications service provider before the notice is given. Should the communications service provider have concerns about the reasonableness, cost or technical feasibility of the obligations to be set out in the notice, these should be raised during the consultation process. At the conclusion of these discussions, any outstanding concerns must be taken into account by the Secretary of State as part of the decision making process.

[25] See section 255(2).

Matters to be considered by the Secretary of State

8.11 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 and its effect on the communications service provider. 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.

8.12 As part of the decision, the Secretary of State must take into account, amongst other factors, the matters specified in section 255(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 necessity of the capability but also the likely benefits.

- 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 255(4)).

- 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.

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

- 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.

8.14 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 limited to those set out in regulations made by the Secretary of State under section 253, as described above.

8.15 Before the notice may be given, a Judicial Commissioner must approve the Secretary of State's decision to give the 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 as to whether the notice is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. In reviewing these conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. In addition, the Judicial Commissioner must review the conclusions 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.)

Giving a notice

8.16 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.

8.17 Section 255(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[26]:

- 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.

8.18 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.

8.19 As set out in section 253(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.

8.20 The notice will also specify the telecommunications services or systems to which the obligations will apply.

[26] See section 255 (6).

8.21 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 relating 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[27]. The duty to comply with a technical capability notice relating to targeted or bulk 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[28].

Disclosure of technical capability notices

8.22 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 that have been given a notice. Should criminals become aware of the capabilities of the intercepting agencies, they may alter their behaviours and change communications service provider, making it more difficult to detect their activities of concern.

8.23 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.[29]

8.24 Section 255(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 might 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 a legal advisor in contemplation of legal proceedings, or for the purpose of those proceedings;
- 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.

[27] See section 255(10)(a)

[28] See section 255(10)(b)

[29] See section 255(8)

Regular review

8.25 Section 256(2) of the Act imposes an obligation on the Secretary of State to 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. This evaluation differs from the process provided for in section 257 of the Act, which permits 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.

8.26 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.

8.27 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.

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

- 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.

8.29 When reviewing a technical capability notice, the Secretary of State must consult the communications service provider in deciding whether the notice remains necessary and proportionate.

8.30 A review may conclude that the notice should continue to remain in force, be varied to add or remove obligations, or be revoked. The relevant communications service provider and the operational agencies will be notified of the outcome of the review.

Variation of technical capability notices

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

8.32 Communications service providers which have been given a technical capability notice must notify the Secretary of State of changes to existing telecommunications services and the development of new services and relevant products in advance of their launch. This will enable the Secretary of State to consider whether it is necessary and proportionate to require the communications service provider company to modify an existing capability or provide a new technical capability on the service.

8.33 Certain changes to services, such as upgrades of systems which are already covered by the existing notice, may be agreed between the Secretary of State and communications service provider in question where the change would not require new obligations to be imposed on the company. However, significant changes to networks or service which necessitate new obligations being imposed on the company will require a variation of the technical capability notice.

8.34 Section 256 of the Act provides that technical capability notices may be varied by the Secretary of State if the Secretary of State considers that the variation is necessary and the conduct required by the variation is proportionate to what is sought to be achieved. Where the variation imposes new obligations on the communications service provider, the decision to vary a notice must be approved by a Judicial Commissioner. Judicial Commissioner approval is not required where a variation removes obligations from the notice.

8.35 There are a number of reasons why a notice might be varied. These include:

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

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

8.37 Before varying a notice, the Secretary of State must consult the communications service provider to understand the impact of the change and must take into account the same factors as when deciding to give a notice, including cost and technical implications.[30] The Government should also consult the intercepting agencies to understand the operational impact of any change to the notice.

8.38 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraphs 8.8 - 8.14 above.

8.39 Once a variation has been agreed by the Secretary of State, and the decision to vary a notice has (where necessary) been approved by a Judicial Commissioner, 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.

[30] See section 255(3)

Revocation of technical capability notices

8.40 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 or if it is no longer reasonable to impose certain obligations on the provider.

8.41 Circumstances where it may be necessary 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.

8.42 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

8.43 A person to whom a notice is given may request a review of any aspect of a technical capability notice should they wish to do so. A person may refer the whole or any part of the notice back to the Secretary of State for review under section 257 of the Act.

8.44 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.

8.45 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.

8.46 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.

8.47 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. Notwithstanding the review, the communications service provider may be required to provide assistance in giving effect to a warrant or authorisation.

Contribution of costs for the maintenance of a technical capability

8.48 Section 249 of the Act recognises that communications service providers incur expenses in complying with requirements in the Act, including notices to maintain technical capabilities under Part 9. The Act, therefore, requires the Secretary of State to have in place arrangements to ensure that providers receive an appropriate contribution to these costs.

8.49 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.

8.50 Any contribution towards these costs must be agreed by the Secretary of State before work is commenced to develop, install, or operate the capability. Furthermore, the Secretary of State must be satisfied that the proposed capability will meet the requirements set out in the notice.

8.51 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, certain staff benefits or arrangements made in line with the terms and conditions of employment, such as bonuses paid to members of staff that are reflective or representative of the company's performance, will be excluded from this category of costs. Such matters are arranged between the employer and employee and the Government does not accept responsibility for such costs. Further details with respect to cost recovery will be available in the handbook provided to all communications service providers who maintain an interception capability.

8.52 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

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

8.54 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 Secretary of State of proposed changes.

8.55 Any communications service provider that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made by the Secretary of State. 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

8.56 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).

8.57 Section 250 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 obtain secondary data. Such systems could operate in respect of multiple powers under the Act.

8.58 Where such systems are developed for use by communications service providers, the Secretary of State 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

8.59 The obligations the Secretary of State considers necessary and proportionate 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, in accordance with section 253(5) of the Act.

8.60 Communications service providers may be obligated to maintain physical, document, operational and non-operational information technology, and personnel security to standards as specified in the notice, subject to guidance from the National Technical Assistance Centre (NTAC). Such obligations may include: implementing the Government's Information Assurance Maturity Model in conjunction with a consultant holding a National Cyber Security Centre recognised certification[31] to identify their level of information security.

[31] For further details, please see guidance on the National Cyber Security Centre's website: www.ncsc.gov.uk

8.61 Specific security requirements will 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.

8.62 . A Service Level Agreement may also be negotiated between the Government and the communications service provider. If given, this document will provide detail of how the obligations imposed by a technical capability notice will be effected, including those that relate to security.

8.63 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.

8.64 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.

8.65 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 considered appropriate by the Secretary of State.

Security

8.66 The following sections provide detail of the security requirements which are likely to be imposed by a technical capability notice. The security arrangements required to protect interception capabilities and interception product 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
- Procedural security e.g. processes and controls.

8.67 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 to ensure compliance with the notice will be agreed in confidence between the Secretary of State and the relevant communications service provider. In practice, the Secretary of State can delegate participation in this exercise to officials. 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.

8.68 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

8.69 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.

8.70 The intercepting agency must be notified of any errors in the interception. NTAC should be notified of any problems or changes to interception capability or the delivery of intercept product.

8.71 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.

8.72 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

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

8.74 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

8.75 Each communications service provider to whom a notice is given 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.

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

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

Personnel security

8.78 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.

8.79 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.

8.80 All persons who may have access to intercepted content or secondary data, 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 security clearance of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed.

8.81 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

8.82 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.

8.83 Equipment used to intercept communications must be sanitised and securely disposed of at the end of its life.[32]

Operations management

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

[32] Please see 8.94 for further details on the disposal of interception systems.

8.85 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.

8.86 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.

8.87 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.

8.88 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.

8.89 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.

8.90 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

8.91 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.

8.92 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.

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

Management of incidents

8.94 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. In addition, a communications service provider must report to the Investigatory Powers Commissioner any relevant error of which it is aware[33].

8.95 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

8.96 The requirement that when destroying data it must be deleted in such a way that it 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.

8.97 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.

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

8.99 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 under this Act or another enactment.

[33] See section 235(6). A relevant error is an error by a public authority in 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. For further detail, please also see Chapter 10.

9 Safeguards (including privileged or confidential information)

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 in a fashion 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 and secondary data is limited to the minimum necessary for the authorised purposes. Sections 46(3) and 132(3) of the Act provide that something is necessary for the authorised purposes if the intercepted content and secondary data:

- 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 in the interests of the economic well-being of the UK so far as those interests are relevant to national security;
- 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 or the Public Records Act (Northern Ireland) 1923.

Exclusion of intercept from legal proceedings, duty not to make unauthorised disclosure and excepted disclosures

9.3 Sections 56 states that no evidence may be adduced, questions asked, assertions or disclosure made in connection with any legal proceedings or Inquiries Act proceedings, which disclose the content or secondary data from interception (where it can be inferred that the information came from interception) or which tends to suggest that interception-related conduct has or may have occurred. This applies to any activity carried out under Chapter 1 of Part 2 of the Act but not to conduct undertaken under Chapter 2 of Part 2. The exclusion also applies to activity which was authorised under Chapter 1 of Part 1 of RIPA or which was an offence under section 1 (or would have been an offence in the absence of subsections 2 and 3) of the Interception of Communications Act 1985.

9.4 Section 57 imposes a duty on those individuals listed in subsection (3) not to disclose the existence or content and secondary data of a warrant, details of the issue of the warrant or any renewal or modification of the warrant, the existence or content of any requirement to provide assistance in giving effect to a warrant, steps taken in pursuance of the warrant or any material obtained under a warrant. Section 59 sets out the offence for an individual who makes an unauthorised disclosure.

9.5 Section 58 of the Act sets out the meaning of “excepted disclosure” and the circumstances in which disclosure made in relation to a warrant is permitted (further information on excepted disclosure can be found in Chapter 11). Section 58 is broken down into a number of types of circumstances (or “heads) in which disclosure would be an “excepted disclosure”.

9.6 **Head 1** includes where it is authorised by the warrant, authorised by the person to whom the warrant is addressed or authorised by terms of any requirement to provide assistance in giving effect to the warrant.

9.7 **Head 2** provides for disclosures to or authorised by a Judicial Commissioner and disclosure to the Independent Police Complaints Commission or the Intelligence and Security Committee of Parliament for the purpose of carrying out their respective functions.

9.8 **Head 3** provides for disclosure by a legal adviser in contemplation of or in connection with any legal proceedings, or disclosure by a professional legal advisor to his or her client, or vice versa, for the purpose of giving advice about relevant provisions (which are described in section 58(7).

9.9 **Head 4** provides for disclosure of statistics by postal or telecommunications operators in accordance with regulations made by the Secretary of State. The regulations may allow the publication of statistics relating to the number of warrants to which they have given effect Head 4 also includes when a disclosure is made, not only in relation to a particular warrant but in relation to interception warrants in general.

9.10 Section 58(5)(a) provides for disclosure by a lawyer for the purpose of legal proceedings. Section 58(5)(b) provides for disclosure by a legal adviser or their client or representatives in connection with giving advice about the operation of Chapter 1 of Part 2, of the Act or Chapter 1 of Part 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 56. The effects of these sections is also that any disclosure to a lawyer by the person listed in section 57(3) must either be for the purposes in section 58(4)(b) or be permissible under one of the other 'Heads' set out in section 58.

9.11 Disclosure may also be subject to other duties of confidentiality, for example, from contractual 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.

Reviewing warrants

9.12 Regular reviews of all warrants should be undertaken during their life time to assess the necessity and proportionality of the conduct. 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 particularly sensitive information is likely to be obtained. As set out at section 2(2)(b) of the Act, at the point the intercepting authority is considering applying for a warrant, they must have regard to whether the level of protection to be applied in relation to information obtained under the warrant is higher because of the particular sensitivity of that information.

9.13 In each case, unless specified by the Secretary of State, 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.

9.14 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.

Dissemination of intercepted content and secondary data

9.15 Intercepted content and secondary data will need to be disseminated both within and between agencies, as well as to consumers of intelligence (which includes oversight bodies, Secretary of State etc.), where necessary in order for action to be taken on it. The number of persons to whom any of the intercepted content or secondary data 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 or secondary data 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 or secondary data to carry out those duties. In the same way, only so much of the intercepted content or secondary data 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.

9.16 The obligations apply not just to the original intercepting authority, 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 or secondary data further. In others, explicit safeguards are applied to secondary recipients.

9.17 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 and 140 of the Act and paragraphs 9.5-9.11 of this Code.

9.18 Sections 52 and 151 of the Act stipulate that where intercepted content and secondary data is disclosed to the authorities of a country or territory outside the UK, the appropriate issuing authority must ensure that intercepted content and secondary data is only handed over to overseas authorities if the following requirements are met:

- It appears to the issuing authority 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 (if any) that the issuing authority considers appropriate;

- Where unselected data obtained under a bulk warrant is disclosed to overseas authorities, it appears to the Secretary of State that requirements corresponding to the requirements of section 142 (safeguards relating to the examination of material) will also apply to the extent (if any) that the Secretary of State considers appropriate; and

- Restrictions are in force which would prevent, to such extent as the appropriate issuing authority 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.

Copying

9.19 Intercepted content and secondary data 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 and secondary data, but also extracts and summaries which identify the material as having been obtained under a warrant, and any record referring to an interception and which is a record of the identities of the persons to or by whom the intercepted content and secondary data was sent or to whom the material relates.

Storage

9.20 All copies, extracts and summaries of intercepted content and secondary data must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. 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.

9.21 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 clearance regime for personnel which is designed to provide assurance that those who have access to this content and secondary data are reliable and trustworthy.

Destruction

9.22 Intercepted content and secondary data, and all copies, extracts and summaries which can be identified as the product of an interception, must be scheduled for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible[34]. 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.

[34] For example, by taking reasonable steps to make the data unavailable or inaccessible to authorised persons. No further steps are required such as physical destruction of hardware.

9.23 Where an intercepting agency undertakes interception under a bulk 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. Where communications are stored on a system, they will not be stored for the purpose of IPC oversight beyond the retention period already set for that system. 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.

9.24 Any collateral material that has been acquired over the course of a testing or training exercise should be destroyed as soon as reasonably possible when the purpose of the testing or training exercise has been fulfilled. For example, it may take a period of time to go through the data to check whether the equipment has worked properly. It may also be appropriate in some cases to retain test data and re-run this rather than cause further intrusion by carrying out further interception.

Safeguards applicable to requesting and handling intercept by overseas authorities other than in accordance with mutual assistance agreements

9.25 Section 9 applies to requests for interception by overseas authorities of communications sent by or intended for an individual who the person making the request believes will be in the in the British Islands at the time of the interception. Such requests may not be made by or on behalf of a person in the United Kingdom unless a targeted interception warrant or a targeted examination warrant has been issued under Chapter 1 of Part 2. This means that when a UK intercepting agency asks an overseas authority to carry out (on its behalf) interception of communications of a person in the UK which the overseas authority would not otherwise have been carrying out, the UK intercepting agency must have an interception warrant in place.

9.26 Where intercepted content or secondary data is obtained by a UK intercepting agency as a result of such a request the intercepted 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 agency as a result of interception under the Act.

Additional rules for requesting and handling unanalysed intercepted communications content and secondary data from overseas authorities

Application of this chapter

9.27 The following paragraphs apply to those intercepting agencies that undertake bulk interception under a Part 6 warrant. These safeguards apply in addition to the requirements of section 9 of the Act and paragraphs 9.25 and 9.26 of the code.

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

9.28 A request may only be made by an intercepting agency to overseas authorities 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 overseas authority 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.

9.29 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 at the time of the interception.

9.30 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 specifying 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 specifying 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 an overseas authority

9.31 If a request falling within the second bullet of paragraph 9.28 is approved by the Secretary of State other than in relation to specific selectors, any content 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 that content by reference to such factors[35].[36]

9.32 Where unanalysed intercepted communications content or secondary data are obtained by the intercepting agencies as set out in paragraph 9.28, 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[37] and secondary data[38] 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 agency as a result of interception under the Act.

9.33 The internal arrangements of the UK intercepting agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflects its nature and intrusiveness. The specific periods should normally be no longer than two years.[39] 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 destroyed. 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.

---

[35] In the event that the communications obtained by virtue of such a request constitute a bulk personal dataset (as defined by section 199), then Part 7 of the Act applies and the intercepting agency should apply the safeguards in Part 7, including the safeguards relating to examination of bulk personal datasets, and not paragraph 9.28 of this Code. In such a case, paragraph 9.29 of this Code should be applied in addition to the safeguards in Part 7 of the Act. Nothing in paragraphs 9.28 or 9.29 disapplies the provisions of Part 7 of the Act.

[36] 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).

[37] Whether analysed or unanalysed.

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

[39] In the event that the data in question constitutes a bulk personal dataset (as defined by section 199), the maximum retention period should be that prescribed by the safeguards in Part 7 rather than the two-year maximum period stipulated in paragraph 9.30 of this Code.

9.34 All requests to an overseas authority for unanalysed intercepted communications (and secondary data), in the absence of a relevant interception warrant issued under the Act will be notified to the Investigatory Powers Commissioner as soon as reasonably practicable.

9.35 Nothing in this section disapplies the provisions of Part 7 of the Act, in relation to Bulk Personal Datasets.

Confidential or privileged information

9.36 Particular consideration should be given to the interception of communications or the selection for examination of content containing information where individuals might reasonably assume a high degree of confidentiality. This includes where the communications contain information that is legally privileged (see paragraphs 9.43 – 9.62); confidential journalistic material or where communications identify a journalists source (see paragraphs 9.68 – 9.77); where communications contain confidential personal information or communications between a Member of a relevant legislature and another person on constituency business (explained below at paragraph 9.39).

9.37 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. Authorised persons in the intercepting agencies should receive appropriate training on the safeguards regarding confidential or privileged information.

9.38 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.

Confidential personal information and communications between a member of a relevant legislature and another person on constituency business

9.39 Where the intention is to acquire confidential personal information, or communications between a member of a relevant legislature (as defined in section 26) and another person on constituency business the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the information is exchanged with the intention of furthering a criminal purpose, for example, if purported spiritual counselling involves incitement to murder or to acts of terrorism, then the information will not be considered confidential for the purposes of the Act. If the acquisition of confidential personal or constituency business 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.

9.40 Where confidential or constituency business information is retained and disseminated to an outside body, reasonable steps should be taken to mark the disseminated 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.

9.41 Any case where confidential or constituency business content is retained, other than for the purposes of destruction, and disseminated, it should be notified to the Investigatory Powers Commissioner as soon as reasonably practicable

9.42 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 or constituency business information and is retained other than for the purpose of its destruction.

Communications subject to legal privilege

9.43 Section 10 of the Police and Criminal Evidence Act 1984 describes those matters that are subject to legal privilege in England and Wales. In Scotland, those matters subject to legal privilege are defined in Section 263 of the Investigatory Powers Act. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

9.44 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the legal adviser is acting unwittingly or culpably). Privilege is not lost where a professional legal adviser is 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 a member of the legal profession, such as advocates, barristers, solicitors or Chartered Legal Executives.

9.45 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 considered in accordance with section 27: 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.

9.46 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.. Section 27 provides for three different circumstances where legally privileged items will or may be obtained or selected for examination. They are; i) where privileged material is likely to be obtained or selected for examination; ii) where privileged material is intentionally sought, or selected for examination; and iii) where the purpose or one of the purposes is to obtain communications that, if they were not made with the intention of furthering a criminal purpose, would be subject to privilege. Further guidance is set out in paragraphs 9.47 to 9.59 below as to what should be done in each of those cases.

Application process for targeted warrants where the communications are likely to include privileged items

9.47 Section 27 of the Act sets out the processes that must be followed where a targeted warrant may obtain or select for examination communications subject to legal privilege. Different processes apply depending on whether intercepting or examining communications subject to legal privilege is the purpose (or one of the purposes) of the warrant, or whether it is not the purpose but is nevertheless likely. Subsections (8) and (9) set out the process where the purpose of the warrant is not to obtain or examine communications subject to legal privilege, but where the intercepting agency considers it likely that the warrant would authorise or require the interception of communications subject to legal privilege, or in the case of an examination warrant, where the warrant would authorise the selection for examination of communications likely to include items subject to legal privilege. In such cases the warrant application must be clear that the warrant would authorise the interception or selection for examination of communications likely to include items subject to legal privilege and must include an assessment of how likely it is that communications which are subject to legal privilege will be intercepted or examined. This is in addition to the application setting out the reasons why it is considered necessary for interception or examination to take place. In the application, 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.

Application process for targeted warrants where the purpose, or one of the purposes, is to obtain or examine legally privileged communications

9.48 Where the intention is to acquire legally privileged communications, the targeted warrant application must contain a statement that the purpose, or one of the purposes, of the warrant is to obtain legally privileged material. Section 27 provides that the warrant may only be issued if the Secretary of State is satisfied that there are exceptional and compelling circumstances that make the warrant necessary, and the Judicial Commissioner approves the decision to issue the warrant. Section 27 also sets out that circumstances cannot be exceptional and compelling unless certain conditions are met. Exceptional and compelling circumstances will arise only in a very restricted range of cases. Section 27 makes clear that a warrant to target such material can only be issued where there is a threat to life or limb, or in the interests of national security. The exceptional and compelling test can only be met when the public interest in obtaining the information sought outweighs the public interest in maintaining the confidentiality of legally privileged material, and when there are no other reasonable means of obtaining the required information. The interception must be reasonably regarded as likely to yield the 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. 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.

9.49 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 and must have regard to the public interest in the confidentiality of items subject to privilege. They will wish to consider carefully whether the activity or threat being investigated is of a sufficiently serious nature to override the public interest in preserving the confidentiality of privileged communications, and the likelihood that the information sought will have a positive impact on the investigation. The Secretary of State must take into account both the public interest in preserving the confidentiality of those particular communications and the broader public interest in maintaining the confidentiality of privileged communications more generally. The Secretary of State must consider that there are exceptional and compelling circumstances that make it necessary to issue the warrant and must be satisfied that there are appropriate arrangements in place for the handling, retention, use and destruction of privileged items, and the Judicial Commissioner must approve the Secretary of State's decision to issue the warrant.. In such circumstances, the Secretary of State will be able to impose additional requirements such as regular reporting arrangements, so as to keep the warrant under review more effectively.

9.50 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.

9.51 Where an application for a warrant is made where the purpose or one of the purposes is to obtain communications that, if they were not made with the intention of furthering a criminal purpose, would be subject to privilege and where the requesting agency considers that the communications are likely to be made to further a criminal purpose, the application must include a statement to that effect and the reasons for believing that the communications are likely to be made to further a criminal purpose. For example, if the requesting agency had reliable intelligence that a criminal fugitive was seeking advice from a lawyer in order to obtain a false alibi or to assist them in evading arrest, then this may provide grounds for an assessment that the communications with the lawyer will not be privileged, notwithstanding the fugitive appeared to be seeking advice from a lawyer in a professional capacity, and this information should be set out in the application. The requirement to ensure the case for a warrant is presented in the application in a fair and balanced way, including information which supports or weakens the case for the warrant which applies to warrant applications (as set out in paragraph 5.8) applies in these circumstances as it does elsewhere. For example, information which may undermine the assessment that communications are likely to be made to further a criminal purpose must also be included in the application to ensure the Secretary of State can make an informed assessment about the nature of the communications. The warrant can only be issued where the Secretary of State considers that the targeted communications are likely to be communications made with the intention of furthering a criminal purpose

9.52 In a case where section 27 (items subject to legal privilege) applies in relation to making a major modification to a warrant, the same safeguards will apply as apply when a warrant is issued.

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

9.53 In line with section 153 of the Act, where the content of communications intercepted under a bulk interception warrant is to be selected for examination according to criteria that are intended to, or are likely to result in, identifying communications subject to legal privilege, the enhanced procedure described at paragraph 9.43 to 9.47 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 paragraphs 9.43 to 9.47.

9.54 An authorised person in an intercepting agency must notify a senior official[40] before using criteria to select any bulk intercepted content for examination, where this will, or is likely to, result in the identification of legally privileged communications. The notification must address the same considerations as described in paragraph 9.36. 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 9.43 to 9.46. The authorised person is prohibited from accessing the content until he or she has received approval from the senior official authorising the selection for examination of communications subject to legal privilege.

[40] Senior official is defined in section 157

9.55 In the event that privileged communications are inadvertently and unexpectedly selected for examination (and where the enhanced procedure in paragraph 9.48 and 9.52 has consequently not been followed), any content so obtained must be handled strictly in accordance with the requirements of section 153 and the provisions of this chapter set out at paragraphs 9.68 to 9.77. No further privileged communications may be intentionally selected for examination by reference to those criteria unless approved by the senior official as set out in paragraph 9.54.

Lawyers' communications

9.56 Where a lawyer, acting in this professional capacity, is the subject of a targeted interception warrant or a targeted examination warrant or where his or her communications are to be selected for examination in accordance with section 153, it is possible that a substantial proportion of the communications which will be intercepted or selected for examination 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 that professional capacity where it is intended that a lawyer's communications are to be intercepted or selected for examination,the intercepting agency must assume that section 27 applies. Intercepting agencies should provide internal guidance to their staff in relation to determining whether a target is a lawyer acting in this professional capacity.

9.57 The intercepting agency will therefore need to consider which of the three circumstances which apply when privileged items will or may be obtained (or selected for examination) is relevant, and what processes should therefore be followed. In other words, they will need to consider whether privileged material is likely to be obtained or selected for examination; whether privileged material is intentionally sought, or selected for examination; or whether the purpose or one of the purposes is to obtain communications that, if they were not made with the intention of furthering a criminal purpose, would be subject to privilege. This paragraph does not prevent an application being made on the grounds that the lawyer is under investigation for serious criminal offences, in which case, the application or notification must be made on the basis that it is likely to acquire communications subject to legal privilege and the additional considerations set out at paragraph 9.47 will apply.

9.58 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

9.59 In addition to safeguards governing the handling and retention of intercepted content as provided for in section 55 of the Act, officials who examine intercepted communications should be alert to any intercepted content which may be subject to legal privilege. Section 55 of the Act sets out the additional arrangements that apply to legally privileged items where the intention is to retain them for a purpose other than their desctruction.

9.60 A legal advisor in the intercepting agency must be consulted when it is believed that material which attracts privilege is to be retained other than for the purpose of destruction. The legal advisor is responsible for assessing the material rather than an authorised person who is involved in an investigation. In cases where there is doubt as to whether material is privileged or not, the Investigatory Powers Commissioner may be informed who will be able to give a view. 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 53(3). If not, the content should not be retained, other than for the purpose of its destruction.

9.61 Content which has been identified as legally privileged (and is being retained for purposes other than its destruction) should be clearly marked as subject to legal privilege and the Investigatory Powers Commissioner must be notified of the retention of the items as soon as reasonably practicable. Paragraph 9.62 provides more detail on reporting privileged items to the Commissioner. 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 54(3). Privileged items must be securely destroyed when their 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, for purposes other than their destruction, remains necessary and proportionate for the authorised statutory purposes.

Reporting to the Commissioner

9.62 In those cases where legally privileged items have been intercepted and retained other than for the purpose of destruction or, in the case of items intercepted in bulk, selected for examination and retained other than for the purposes of destruction, the matter should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable.

9.63 Section 55 provides that the Commissioner must order the destruction of the material or impose conditions on its use or retention unless the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. Even if retention is necessary and the public interest in its retention outweighs the public interest in the confidentiality of items subject to legal privilege, the Commissioner may still impose conditions as the Commissioner considers necessary to protect the public interest in the confidentiality of items subject to privilege. It may be the case in some circumstances that privileged material can be retained when its retention does not outweigh the public interest in the confidentiality of items subject to privilege. This includes, for example, where it is not possible to separate privileged items from those that are not privileged and of intelligence value and where the retention is necessary and proportionate for one of more of the authorised purposes set out in section 53(3). In these circumstances, the Commissioner must impose conditions on the use or retention of the item.

9.64 The Investigatory Powers Commissioner will make an assessment of whether the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and of whether retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. If both of those conditions are met, then the Commissioner may impose conditions as to the use or retention of the items, but the Commissioner is not obliged to do so. If those conditions are not met, the Commissioner must direct that the item is destroyed, or must impose one or more conditions as to the use or retention of the items. Circumstances in which it may be appropriate to impose conditions on the use or retention of the item, but not to order destruction of the item, include where it is not possible to separate privileged items from those that are not privileged and of intelligence value, and where the retention is necessary and proportionate for one or more of the authorised purposes set out in section 53(3). The Commissioner must have regard to any representations made by the intercepting agency about the proposed retention of privileged items or conditions that may be imposed.

Dissemination

9.65 In the course of an investigation, an intercepting agency will not act on or further disseminate legally privileged items unless it has first informed the IPC that the items have been obtained or selected for examination, except in urgent circumstances. Where there is an urgent need to take action and it is not reasonably practicable to inform the IPC that the material has been obtained, or selected for examination before taking action, the agency may take action before informing the IPC. In such cases, the agency should, wherever possible consult a legal adviser. An Intercepting agency must not disseminate privileged items if doing so would be contrary to a condition imposed by the IPC in relation to those items.

9.66 The dissemination of legally privileged content to an outside body should be accompanied by a clear warning that it is subject to legal privilege, where doing so would not breach the duty not to disclose the existence or contents of a warrant in section 57 (see paragraph 9.4) . 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.

9.67 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 would yield a litigation advantage, the direction of the Court must be sought.

Applications to intercept communications relating to confidential journalistic material and journalists sources

9.68 There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously.

9.69 Section 264 of the Act defines confidential journalistic material as:

a) In the case of material contained in a communication, journalistic material which the sender of the communication

i. Holds in confidence, or

ii. Intends the recipient, or intended recipient, of the communication to hold in confidence;

b) In any other case, journalistic material which a person holds in confience

9.70 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.

9.71 Section 264(7) sets out when a person holds material in confidence. This is if a person holds material subject to an express or implied undertaking to hold it in confidence or the person holds the material subject to a restriction on disclosure or an obligation of secrecy contained in an enactment. Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist or the source (for example, a news editor who has been sent some notes by a journalist).

9.72 Section 28 sets out the safeguards which apply when an intercepting authority applies for a warrant under Part 2 where the purpose, or one of the purposes, of the warrant is to authorise the interception of communications, or the selection for examination of material, that the authority believes will be confidential journalistic material. The warrant application must contain a statement that the purpose is to authorise or require the interception of (or select for examination) communications which the intercepting authority believes will contain confidential journalistic material. The person to whom the application is made may issue the warrant only if they consider that appropriate safeguards relating to the handling, retention use and disclosure of the material are in place.

9.73 A source of journalistic information is an individual who provides material intending the recipient to use it for the purpose of journalism or knowing that it is likely to be so used. Throughout this code any reference to sources should be understood to include any person acting as an intermediary between a journalist and a source.

9.74 Section 29 sets out the safeguards which apply when an intercepting authority applies for a warrant under Part 2 where the purpose, or one of the purposes is to identify or confirm a source of journalistic information. The application must contain a statement confirming that this is the purpose (or one of the purposes) for the application. The person to whom the application is made may issue the warrant only is they consider that appropriate safeguards relating to the handling, retention, use and disclosure of the material are in place. Communications data alone may not be sufficient to identify a source - consequential action and other information is likely to be required. Identifying communications addresses does not in itself provide sufficient information to determine the nature of a relationship.

9.75 An assessment of whether someone is a journalist (for the purposes of the Act)should be made on all the facts and circumstances available at the time. Consideration should be given, in particular, to the frequency of the individual's relevant activities, the level of personal rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest.

9.76 The interception and examination of communications under Part 2 and Chapter 1 of Part 6 of the Act may be a justifiable interference with an individual's human rights under Articles 8 (right to respect for private and family life) and, in certain circumstances, 10 (freedom of expression) of the European Convention on Human Rights only if the conduct being authorised is necessary, proportionate and in accordance with law.

9.77 Where material is created or acquired with the intention of further a criminal purpose, section 264(5) states that the material is not to be regarded as having been created or acquired for the purpose of journalism. For example, if a terrorist organisation is creating videos for the promotion or glorification of terrorism according to the UK legal standard, the material cannot be regarded as journalistic material for the purposes of the Act and will not attract the safeguards set out in section 28 and 155. Once material has been broadcast, no confidentiality can attach to the material so it is not confidential journalistic material. (The Act in any case makes clear in section 5(1) that acquiring a communication broadcast for general reception is not interception.) The fact that a person uses social media tools to communicate does not, in itself, indicate that that person is a journalist or that he or she is likely to be holding confidential journalistic material as defined in the Act.

Selection for examination of intercepted content or secondary data obtained under a bulk interception warrant, where the purpose or one of the purposes is to identify a journalist's source or to obtain confidential journalistic material

9.79 Where an authorised person in an intercepting agency intends to select for examination content intercepted under a bulk interception warrant in order to identify or confirm a source of journalistic information (and other than where paragraphs [on Targeted applications] apply), he or she must notify a senior official[41] before selecting that content for examination. The senior official, who must not be a member of the intercepting agency to whom the bulk interception warrant is addressed, may only approve the proposed selection for examination if he or she considers that the Agency has arrangements in place for the handling, retention, use and destruction of communications that identify sources of journalistic information. The authorised person is prohibited from selecting the material for examination until he or she has received approval from the senior official authorising the selection of content identifying or confirming a source of journalistic information.

9.80 Secondary data alone may not be sufficient to identify a source – consequential action and other information is likely to be required. Identifying, for example, communications addresses does not in itself provide sufficient information to determine the nature of a relationship. However, where selection is carried out with the intention that the information obtained will be used as part of the assessment of the identity of a source, this will require senior official authorisation in line with the process at paragraph 9.35.

9.81 Where an authorised person in an intercepting agency intends to select content for examination which the agency believes is confidential journalistic material (and other than where paragraphs [on Targeted applications] apply), the authorised person in the intercepting agency must notify a senior official[42] before selecting any content for examination. The senior official, who must not be a member of the intercepting agency to whom the bulk interception warrant is addressed, may only approve the proposed selection for examination if he or she considers that the agency has arrangements in place for the handling, retention, use and destruction of communications that contain confidential journalistic material. The authorised person is prohibited from selecting the material for examination until he or she has received approval from the senior official.

Reporting to the Commissioner

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

[41] Senior official is defined in section 145

[42] Senior official is defined in section 145

9.83 In those cases where content containing confidential journalistic material, or that identify a source of journalistic information, have been intercepted and retained other than for the purpose of destruction - or, in the case of bulk interception, where content containing confidential journalistic material, or communications that identify a source of journalistic information, have been selected for examination and retained other than for the purposes of destruction - the matter should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable.

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 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 or modifications to those warrants;
- All warrant Instruments, associated schedules, renewal instruments and modification instruments (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 and secondary data 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 secondary data) and section 51(5) (destruction of intercepted content and secondary data) are to be met.

10.3 The Secretary of State must keep records of the warrant authorisation process. This should 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.
- A record of whether, following a refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner.
- Where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given.

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 decisions to issue a targeted warrant that a Judicial Commissioner refused to approve.
- 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 approve the decision to issue a targeted warrant.
- The number of decisions to issue a targeted warrant that were refused by the Investigatory Powers Commissioner, following a referral from the Secretary of State.
- The number of targeted warrants issued by the Secretary of State and approved by a Judicial Commissioner.
- The number of targeted warrants issued by the Secretary of State in an urgent case.
- The number of targeted warrants issued by the Secretary of State in an urgent case where a Judicial Commissioner subsequently refused to approve the decision to issue the warrant.
- The number of renewals to targeted warrants that were made.
- The number of targeted warrants that the Secretary of State or Judicial Commissioner refused to approve the renewal of;
- 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 statutory 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 decisions to issue a bulk interception warrant that a Judicial Commissioner refused to approve.
- 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 approve the decision to issue a bulk interception warrant.
- The number of decisions to issue a bulk interception warrant that were refused by the Investigatory Powers Commissioner, following a referral from the Secretary of State.
- 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 the Secretary of State or Judicial Commissioner refused to approve the renewal of;
- 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 operational purposes 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 a Judicial Commissioner refused to approve.
- 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 approve the decision modify a bulk interception warrant.

10.9 These records must be sent in written or electronic form to the Investigatory Powers Commissioner, as requested by the Commissioner. Guidance on record keeping may 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. Proper application of the Investigatory Powers Act 2016 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 a public authority, communications service provider or other persons assisting in giving effect to a warrant.

10.11 Wherever possible, technical systems should incorporate functionality to minimise errors. A person holding a senior position within each intercepting agency must undertake a regular review of errors.

10.12 Section 231(9) of the Act sets out what is meant by a “relevant error”, and section 235(6) requires that any relevant error of which a public authority or communications service provider is aware must be reported to the Investigatory Powers Commissioner.

10.13 Section 231(9)(a) makes clear that an error can only be a relevant error where it is one that has been made by a public authority in complying with any requirements imposed by the Act (or any other enactment), which are subject to review by the Investigatory Powers Commissioner. Section 231(9)(b) sets out that a relevant error must also be one of a description outlined in a Code of Practice under Schedule 7 of the Act. In relation to interception a relevant error is one that meets the description at paragraph 10.15 and, where applicable, 10.14.

10.14 Where interception is authorised under a targeted or bulk interception warrant, a relevant error can only occur after the interception, or the obtaining of secondary data, has commenced. Where selection for examination is authorised under a targeted examination warrant, a relevant error can only occur after that selection has commenced.

10.15 A relevant error may only occur in one or more of the following circumstances:

- The interception of communications without lawful authority has occurred;[43]
- The obtaining of secondary data not in accordance with a warrant under Chapter 1 of Part 2 or Chapter 1 of Part 6 has occurred;
- There has been a failure to adhere to the additional safeguards set out at sections 26 to 29 of the Act;
- There has been a failure to adhere to the restrictions on use or disclosure of material imposed by sections 53 to 55 and sections 150 to 154 of the Act;

10.16 The following provides a non-exhaustive list of possible relevant errors by a public authority in complying with the requirements imposed on it[44] that would fall within the description of a relevant error at paragraph 10.14 and 10.15:

- Human error, such as incorrect transposition of communications addresses or identifiers which leads to the wrong intercepted content being intercepted or secondary data obtained;
- 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 held by the intercepting agency at the time of seeking a warrant could reasonably have indicated this.
- Failure to cease interception when the interception warrant has been cancelled;
- A breach of the relevant safeguard section caused by software or hardware errors;
- Selection for examination of bulk intercepted content or secondary data without a valid Operational Purpose;

[43] For the purposes of this section, interception without lawful authority is a failure for a public authority to have in place lawful authority to conduct interception, in accordance with section 6 of the Act, and where the exercise of that interception, were it lawfully authorised, would be a matter which the Investigatory Powers Commissioner would have oversight of under section 229 of the Act.

[44] In accordance with s231(9)(a).

- Retention of data when it is no longer necessary for the authorised purposes;

- Selection for examination of content by a factor or criteria refereable to an individual known to be in the British Islands that is not authorised by a Targeted Examination Warrant or written authorisation under s152(5);

- A public authority selects for examination an item subject to legal privilege, using criteria designed to identify material subject to legal privilege, without complying with the requirements of section 153;

- A public authority fails to inform the IPC that it has intercepted, or has selected for examination, an item which is legally privileged or which contains confidential journalistic material, and intends to retain it for purposes other than its destruction;

10.17 The description of relevant errors at 10.14 and 10.15 captures those circumstances where an error will involve an interference with privacy. Such errors can have very significant consequences on an affected individual's rights and that is why the Act requires that all relevant errors must be reported to the Investigatory Powers Commissioner by the public authority or communications service provider that is aware of the error.

10.18 When a relevant error has occurred, the public authority that made the error must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance processes that a relevant 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.

10.19 From the point at which the public authority identifies that a relevant error may have occurred, they must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the intercepting agency must also inform the Commissioner of when it was initially identified that an error may have taken place.

10.20 Section 235(6) of the Act also places a requirement on communications service providers to report to the Investigatory Powers Commissioner any relevant error, committed by a public authority, of which they become aware. In such circumstances, the process for reporting the error to the Investigatory Powers Commissioner at paragraphs 10.18 and 10.19 above applies to communications service providers as it applies to public authorities. In addition, the communications service provider should inform the relevant public authority as soon as they become aware that authority may have made an error. The communications service provider may then work in conjunction with the public authority to confirm the fact of the error and report it to the Investigatory Powers Commissioner.

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 and, where it has not been possible to provide the full report within ten working days of establishing the fact of the error, the reasons this is the case. Where the report is being made by the public authority that made the error, that report should also include: the cause of the error; 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.

10.22 As set out at section 231(9) of the Act, the Investigatory Powers Commissioner will keep under review the definition of relevant errors. The Investigatory Powers Commissioner may also issue guidance as necessary, including guidance on the format of error reports.

10.23 An error that falls within the descriptions provided at paragraph 10.15 but is committed either by a communications service provider or any other person providing assistance with giving effect to a warrant is not a relevant error, given that section 231(9)(a) makes clear that a relevant error must be one that is made by a public authority. However, such errors may still cause a significant interference with an individual's rights. As such, in addition to the requirement in the Act to report relevant errors to the Investigatory Powers Commissioner, a public authority or communications service provider should also report to the Investigatory Powers Commissioner any error of which they become aware that meets the criteria at paragraph 10.15 of this section. The reporting of such errors will help to draw attention to those aspects of the interception process that require improvement to eliminate further errors and the undue interference with any individual's rights.

10.24 If a public authority discovers a communications service provider error (which cannot therefore be a relevant 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. For example, if an intercepting agency have instructed a communication service provider to cease interception and have cancelled their warrant but the communication service provider has not terminated the activity.

10.25 Paragraph 14 of Schedule 10 of the Act ensures that where a communications service provider is notifying the Investigatory Powers Commissioner of a personal data breach in accordance with this code of practice – such as in relation to the reporting of an error – the provisions of regulation 5A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 do not apply in relation to that data breach. Those provisions relate to the notification of the data breach to the Information Commissioner and to the subject of the breach.

10.26 In addition to errors, as described in this section, situations may arise where a 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 an overseas intelligence agency 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 relied in good faith. Whilst these actions do not constitute a relevant error on the part of the agency which acted on the information, such occurrences should be brought to the attention of the Investigatory Powers Commissioner.

10.27 Where an error occurs which is also considered to constitute an offence detailed in Chapter 3 of this code, the provisions of this chapter must still be applied to the handling of the error.

Serious errors

10.28 Section 231 of the Act states that the Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Investigatory Powers Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Investigatory Powers Commissioner may not decide that an error is a serious error unless he or she considers 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.

10.29 In deciding whether it is in the public interest for the person concerned to be informed of the error, the Investigatory Powers 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.

10.30 Before making his or her decision, the Investigatory Powers Commissioner must ask the intercepting agency which has made the error to make submissions on the matters concerned.

10.31 When informing a person of a serious error, the Investigatory Powers 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 Investigatory Powers 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 and secondary data in the context of legal 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 and secondary data 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 and secondary data 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. Intercept material is excluded from the initial duty of a prosecutor to disclose information under section 3 of the Criminal Procedure and Investigations Act 1996. For further information on disclosure to a prosecutor and obligations to ensure fairness of proceedings, please see paragraphs 11.5 to 11.10.

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 and secondary data 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 or secondary data to which he or she is given access under paragraph 21(1)(a) to mount a cross-examination, or to do anything other than determine what is required of the prosecutor to secure the fairness of the proceedings.

11.7 The exception does not mean that intercepted content and secondary data should be retained against a remote possibility that it might be relevant to future proceedings. The normal expectation is still for the intercepted content and secondary data to be destroyed in accordance with the general safeguards provided by section 51. The exceptions only come into play if such content and secondary data 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 only gathering evidence for the purpose of a prosecution (although it may be used to help gather other information which can be used in evidence), content and secondary data 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 or secondary data remains in existence.

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

11.9 If intercepted content or secondary data 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 or secondary data of possible relevance to the case has been intercepted.

11.10 Having had access to the content or secondary data, 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 or secondary data 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 and secondary data, where there are exceptional circumstances making that disclosure essential in the interests of justice.[45]

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

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 or secondary data 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 rare step. The Act only allows it where the judge considers it essential in the interests of justice.

11.14 Nothing in these provisions allows intercepted content or secondary data, 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 or secondary data 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 or secondary data to be made to counsel to an inquest and to the solicitor to an inquest. In such cases, counsel or the solicitor should 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 or secondary data 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 or secondary data 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 or secondary data exists in a given case but it would not include disclosure of the intercept content or secondary data. Although disclosure is permitted to the Coroner, no further disclosure is permitted by this section. A coroner notified that intercept content or secondary data may exist in a given case would be prohibited from any further disclosure by section 54(3)(f).

Disclsoure in other civil proceedings

11.19 Schedule 3 to the Act also sets out the other circumstances where content or secondary data obtained under an interception warrant may be used in civil proceedings. This includes (but is not limited to):

- where the interception was carried out under sections 44 to 52 of the Act (or equivalent provisions under the Regulation of Investigatory Powers Act 2000 or the Interception of Communications Act 1985);
- Proceedings linked to executive actions (such as Terrorism Prevention and Investigation Measures, hearings before the Special Immigration Appeals Commission, Proscribed Organisations Appeal Commission or proceedings relating to terrorist asset freezing);
- Closed material proceedings under the Justice and Security Act 2013;
- Proceedings relating to prison release in Northern Ireland; and
- Employment or industrial tribunal proceedings.

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 postal or telecommunication providers or by organisations, including intercepting authorities, for administrative, monitoring and record keeping purposes;
- Where it is carried out for enforcement purposes by an officer of Her Majesty's Revenue and Customs under section 159 of the Customs and Excise Management Act 1979, as applied by Section 105 of the Postal Services Act 2000 or that section and another enactment;
- Where it is carried out by OFCOM in connection with wireless telegraphy;
- 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, an EI warrant under Part 5 or a Court order;
- In Prisons, immigration detention facilities or psychiatric hospitals in accordance with relevant rules or directions; or
- In accordance with certain overseas requests.

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 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

12.4 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.

12.5 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 the 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[46], or their RIPSA equivalents.

Interception by providers of postal or telecommunications services

12.6 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 provision or 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 postal or telecommunications 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 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

12.7 Section 44 of the Act enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept communications.

Regulations made under section 46 may allow conduct necessary for businesses for a range of purposes, including the monitoring of productivity and the detection of offences by employees. For example, they may allow the monitoring or recording of telephone calls to a call centre. Regulations may also allow the government to protect national security, for example to test and assure the security of their own systems from cyber-attack. The Regulations recognise that an interception warrant is not needed when conduct of this nature is authorised by the Regulations.

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

12.8 Regulations made under section 46 may also be used in the Cyber Security context to authorise conduct to protect critical national infrastructure (CNI) and public sector organisations. This would enable the Government to undertake on-going protective monitoring of UK organisations in order to learn about and scan for potential cyber-attacks. Were Regulations made under section 46 used in this way, they would require consent from system controllers to ensure that organisations 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

12.9 Section 50 of the Act permits a communications service provider to intercept communications at the request of an authority in a country with which the UK has a relevant international agreement. The request must meet the requirements of the agreement under which it is submitted. The interception may only be carried out by the Communications Service Provider only if the purpose it to obtain information about someone outside the Uk and whom both the both the Communications Service Provider and the authority making the request believe is outside the UK.

12.10 The Secretary of State must designate those international agreements to which section 50 applies. The Secretary of State may also make regulations which set out further conditions which must also be met before Communications Service Provider responds to a request under this section.

12.11 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

12.12 Under section 4(4)(b) of the Act, accessing the contents of a communication stored in or by the 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 statutory provisions that authorise access to stored communications other than an interception warrant (see paragraph 12.13). 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).

12.13 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.

12.14 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 to access or obtain content include (but are not limited to) the following:

- Powers of search, seizure or production 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

12.15 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, for example, gather evidence of offences, safeguard children and protect the public.

12.16 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 includes providing 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 (the 'Technical Advisory Panel').

13.2 The 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 Commissioner may undertake these inspections, as far as they relate to the Commissioner's statutory functions, entirely on his or her own initiative or they may be asked to investigate a specific issue by the Prime Minister. Section 236 also provides for the Intelligence and Security Committee of Parliament to refer a matter to the Commissioner with a view to carrying out an investigation, inspection or audit.

13.3 The Commissioner 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 Commissioner 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 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 both the UK Parliament and the Scottish 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.

13.7 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.

13.8 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 consider and determine complaints regarding public authority use of certain investigatory powers, including those covered by this code, as well as conduct by or on behalf of any of the intelligence agencies and is the only appropriate tribunal for human rights claims against the intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

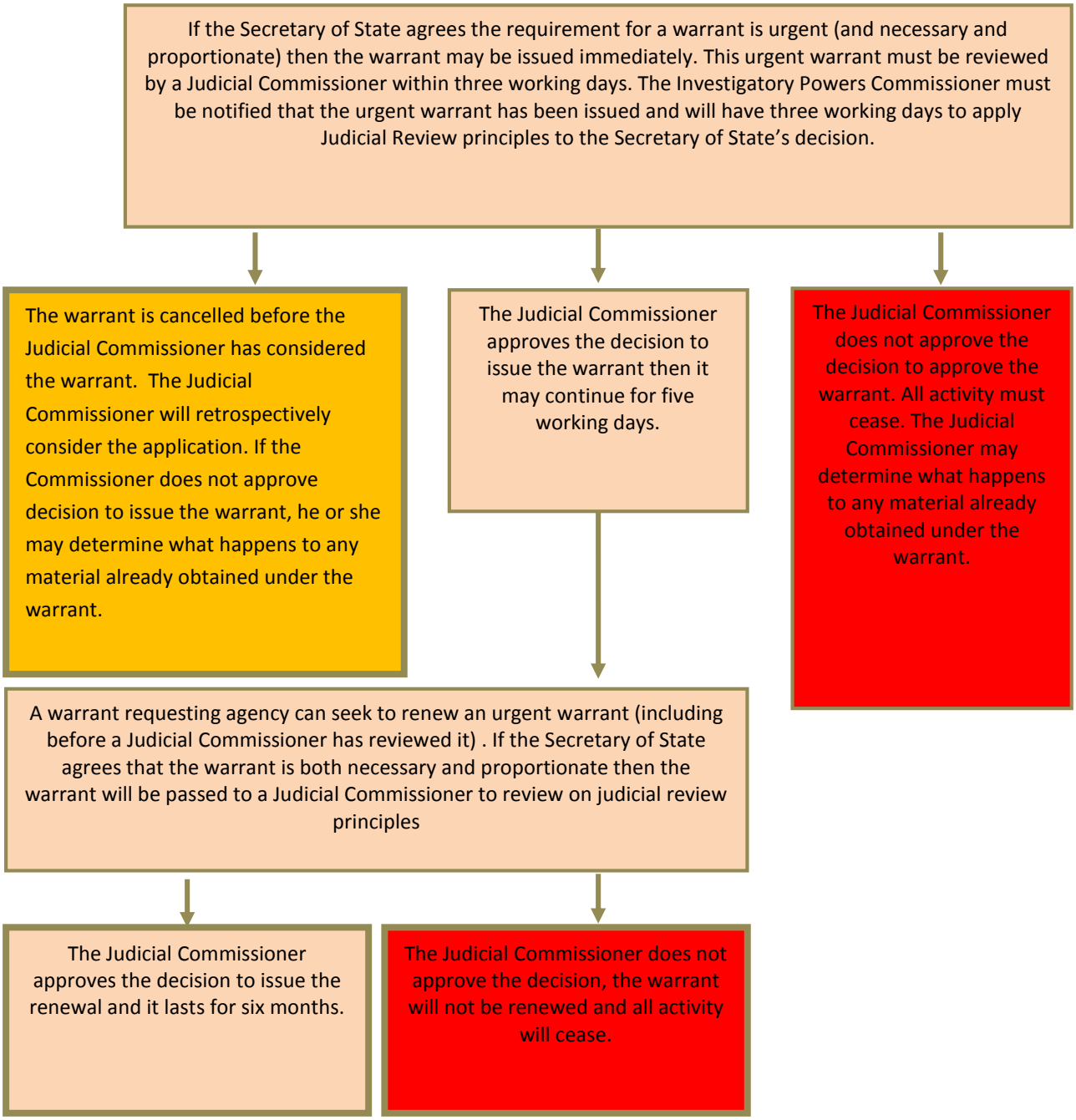
14.2 The IPT is entirely independent from Her Majesty's Government and the public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information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