Equipment Interference

DRAFT Code of Practice

July 2017

Scottish Government
Riaghaltas na h-Alba
gov.scot

Equipment Interference
DRAFT Code of Practice

Pursuant to Section 24 of the Regulation of Investigatory Powers (Scotland) Act 2000

Contents

1	**Introduction**	**2**
2	**Scope and Definitions**	**4**
3	**Targeted Equipment Interference Warrants**	**9**
4	**Implementation of Warrants and Communications Service Provider Compliance**	**29**
5	**Handling of Information, General Safeguards and Sensitive Professions**	**30**
6	**Record-keeping and Error Reporting**	**41**
7	**Oversight**	**45**
8	**Complaints**	**46**

Annex A: Schedule 6: Issue of warrants under section 101 etc to whom this code applies

1 Introduction

Background

1.1 This code of practice provides guidance on targeted equipment interference by the Police Service of Scotland and the Police Investigations and Review Commissioner. Throughout the remainder of this code, these bodies will be referred to as the "relevant agencies." The Investigatory Powers Act 2016 (the Act) provides a statutory framework for authorising equipment interference when the European Convention of Human Rights ("the ECHR") and/or the Computer Misuse Act 1990 ("the CMA") are likely to be engaged. Chapter 2 of this code provides further guidance on the CMA, and when targeted equipment interference warrants are required under the Act.

1.2 This code is issued pursuant to section 24 of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A), which provides that the Scottish Ministers shall issue one or more codes of practice relating to the exercise and performance of powers and duties conferred or imposed by or under a number of Acts, including part 5 of the 2016 Act, so far as it relates to the relevant agencies.

1.3 This code is publicly available and should be readily accessible by members of any of the equipment interference agencies seeking to use the Act to authorise equipment interference.

1.4 For the avoidance of doubt, the guidance in this code takes precedence over any contrary content of a relevant agency's internal advice or guidance.

1.5 Further guidance relating to equipment interference can also be obtained in the Equipment Interference Code of Practice issued by the Home Office, which provides, among other things, information pertaining to the obtaining of warrants from the Scottish Ministers by the security and intelligence agencies.

Effect of code

1.6 Section 26 of RIP(S)A provides that all codes of practice in force at any time under RIP(S)A are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal, including the Investigatory Powers Tribunal ("the IPT") established under the Regulation of Investigatory Powers Act 2000 ("RIPA"), or to a supervisory authority[1] exercising functions under the Act, it must be taken into account. The relevant agencies may also be required to justify, with regard to this code, the use of targeted equipment interference warrants in general or the failure to use warrants where appropriate.

1.7 Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are not provisions of the code, but are included for guidance only. It is not possible for theoretical examples to replicate the level of detail to be found in real cases. Consequently, the relevant agencies should avoid allowing superficial similarities with the examples to determine their decisions and should not seek to justify their decisions solely by reference to the examples rather than to the law, including the provisions of this code. The examples should not be taken as confirmation that any particular relevant agency undertakes the activity described; the examples are for illustrative purposes only.

[1] A supervisory authority is the IPC or any other Judicial Commissioner.

Equipment interference to which this code applies

1.8 Part 5 of the Act provides for the issue of targeted equipment interference warrants authorising interference with any equipment for the purpose of obtaining communications, equipment data or other information.

1.9 Targeted equipment interference warrants may authorise both physical interference (e.g. covertly downloading data from a device to which physical access has been gained) and remote interference (e.g. installing a piece of software on to a device over a wired and/or wireless network in order to remotely extract information from the device).

1.10 A targeted equipment interference warrant provides lawful authority to carry out the acquisition of communications stored in or by a telecommunications system.

1.11 Chapters 2 and 3 of this code provide a description of targeted equipment interference activities and the circumstances when a targeted equipment interference warrant is required, along with definitions of terms, exceptions and examples.

Basis for lawful equipment interference activity

1.12 The Human Rights Act 1998 gives effect in UK law to the rights set out in the ECHR. Some of these rights are absolute, such as the prohibition on torture, while others are qualified, which means that it is permissible for public authorities to interfere with those rights if certain conditions are satisfied.

1.13 Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when the equipment interference agencies seek to obtain personal information about a person by means of equipment interference. Such conduct may also engage Article 1 of the First Protocol (right to peaceful enjoyment of possessions[2]).

1.14 The use of targeted equipment interference techniques may require interference with computers. Interfering with the functions of a computer or otherwise accessing it where there is no lawful authority to do so may, in certain circumstances, amount to a criminal offence. The offences related to unauthorised interferences with computers are set out in the CMA and are explained further in Chapter 2 of this code.

1.15 Part 5 of the Act provides a statutory framework under which equipment interference activities which engage the ECHR and/or would otherwise constitute an offence under the CMA can be authorised and conducted lawfully.

[2] Including equipment.

2 Scope and definitions

Overview

2.1 This chapter provides guidance on the scope of targeted equipment interference and relevant definitions, and on the circumstances where a targeted equipment interference warrant is required for a relevant agency to undertake related activity.

2.2 Targeted equipment interference describes a range of techniques that may be used by the relevant agencies to obtain communications, equipment data or other information from the equipment. The material so obtained may be used evidentially or as intelligence, or in some cases to test, maintain or develop equipment interference capabilities.

2.3 Targeted equipment interference operations vary in complexity. The relevant agencies may covertly download data from a subject's mobile device when it is left unattended, or they may use someone's login credentials to gain access to data held on a computer. More complex targeted equipment interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device.

2.4 For the purposes of the Act, a targeted equipment interference warrant can only be obtained for the purposes of obtaining communications, equipment data or other information.

2.5 Interference with equipment that is not for the purpose of acquiring communications, equipment data or other information will continue to fall within the definition of 'property interference' for the purposes of the Covert Surveillance and Property Interference Code of Practice. For example, disabling an alarm system to allow covert access to a building does not constitute equipment interference, although it may be necessary to interfere with the alarm system (equipment) to acquire equipment data in order to understand the alarm's operating system to enable it to be disabled. In such circumstances, the purpose of the interference is to defeat the alarm system and the acquisition of the equipment data is incidental. To the extent such activities would otherwise be unlawful, it should continue to be authorised under Part 3 of the Police Act 1997 ("the 1997 Act").

2.6 This distinction has been drawn so that the Act can apply tailored safeguards, handling arrangements and oversight to activity where the purpose of the interference is to acquire communications, equipment data or other information from equipment. Different considerations, safeguards and legislation will apply where the purpose of the interference does not fall within those categories.

Equipment

2.7 Equipment is defined in section 135 of the Act. "Equipment" comprises any equipment producing "electromagnetic, acoustic or other emissions" and any device capable of being used in connection with such equipment. "Equipment" for these purposes is not limited to equipment which is switched on and/or is emitting signals but also includes equipment which is capable of producing such emissions.

2.8 The definition of equipment is technology neutral. Examples of the types of equipment captured by the definition include devices that are "computers" for the purposes of the CMA, such as desktop computers, laptops, tablets, smart phones, other internet-enabled or networked devices and any other devices capable of being used in connection with such equipment. Cables, wires and storage devices (such as USB storage devices, CDs or hard disks drives) are also covered as they can also produce "emissions" in the form of an electromagnetic field.

Equipment data

2.9 A targeted equipment interference warrant may authorise the obtaining of communications, equipment data and other information. A warrant may also provide for the obtaining of only equipment data. Equipment data comprises:

- systems data which is comprised in, included as part of, attached to or logically associated with the communications or information being acquired; and
- identifying data which is comprised in, included as part of, attached to or logically associated with the communications or information, which is capable of being logically separated from the remainder of the communication or item of information and which, once separated, does not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication or item information.

2.10 Equipment data is defined in section 100 of the Act. Equipment data includes:

- **Systems data**
    - systems data includes two types of data. It includes the data which (when a communication is transmitted via a telecommunications system) is comprised in, attached to or logically associated with that communication and is necessary for the telecommunications system to transmit the communication. Second, there is other data comprised in, attached to or logically associated with communications or items of information which enable systems or services to function. While this second type of systems data is not necessary for a transmission system to transmit a communication, it is also not content. These two types of data make up the broader set of information which is called systems data[3].
    - examples of systems data would be:
        - messages sent between items of network infrastructure to enable the system to manage the flow of communications;
        - router configurations or firewall configurations;
        - software operating system (version);
        - historical contacts from sources such as instant messenger applications or web forums;
        - alternative account identifiers such as email addresses or user IDs; and
        - the period of time a router has been active on a network.
- **Identifying data:**
    - a communication or item of information may include data which may:
        - be used to identify, or assist in identifying, any person, apparatus, system or service;
        - be used to identify any event; or
        - be used to identify the location of any person, event or thing.

[3] Systems data that is necessary for the provision and operation of a service or system also includes the data necessary for the storage of communications and other information on relevant systems. Systems data held on a relevant system may be obtained via an equipment interference warrant under Part 5 of the Act.

- In most cases this data will be systems data. There will, however, be cases where this information does not enable or otherwise facilitate the functioning of a service or system and therefore is not systems data. Where such data can be logically separated from the remainder of the communication or item of information and does not, once separated, reveal anything of what might reasonably be considered to be the meaning (if any) of any communication or item of information (disregarding any inferred meaning) it is identifying data.
- Examples of such data include:
  - the location of a meeting in a calendar appointment;
  - photograph information - such as the time/date and location it was taken; and
  - contact 'mailto' addresses within a webpage.

Communications service provider

2.11 There are obligations under Part 5 of the Act which apply to telecommunications operators. Throughout this code, communications service provider ("CSP") is used to refer to a telecommunications operator.

2.12 A telecommunications operator is a person who offers or provides a telecommunication service to persons in the UK or who controls or provides a telecommunications system which is (in whole or in part) in or controlled from the UK. This definition makes clear that obligations in the Act cannot be imposed on CSPs whose equipment is not in or controlled from the UK or who do not offer or provide services to persons in the UK.

2.13 Section 261 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 telecommunications system (whether or not one provided by the person providing the service); and defines 'telecommunications system' to mean any system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. The definition of 'telecommunications service' in the Act is intentionally broad so that it remains relevant for new technologies.

2.14 The Act makes clear that any service which consists of or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunications system are 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.

2.15 The definition of a telecommunications operator also includes application and website providers but only insofar as they provide a telecommunications service. For example, an online market place may be a telecommunications operator as it provides a connection to an application/website and because it provides a messaging service.

2.16 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.

Restrictions on interference with equipment - Computer Misuse Act 1990

2.17 Interfering with the functions of a computer and accessing its data or its programs, where there is no lawful authority to do so, may in certain circumstances amount to a criminal offence.

Section 14 of the Act imposes restrictions on the relevant agencies, where it is considered that the proposed conduct would constitute one or more offences under sections 1 to 3A of the CMA. Accordingly, it is important that the relevant agencies understand when a CMA offence is likely to be committed.

2.18 "Computer" is not defined in the CMA; rather the Act relies on the ordinary meaning of the word in the relevant context.

2.19 The offences relating to unauthorised interferences with computers are summarised below.

- Section 1: unauthorised access to computer material
- Section 2: unauthorised access with intent to commit or facilitate commission of further offences
- Section 3: Unauthorised acts with intent to impair, or with recklessness as to impairing the operation of a computer
- Section 3ZA: Unauthorised acts causing, or creating risk of, serious damage
- Section 3A: Making, supplying or obtaining articles for use in an offence under section 1, 3 or 3ZA.

2.20 The CMA provides that access will not be 'unauthorised' and an offence will not be committed if the conduct in question takes place pursuant to a relevant authorisation.

Mandatory use of targeted equipment interference warrants: Restrictions on interference for the relevant agencies

2.21 Whether a targeted equipment interference warrant is available or required will depend on a number of factors, including whether the CMA is engaged, the relevant agencies making the application, the nature of the targeted equipment interference, where the interference is taking place and where the conduct takes place from.

2.22 By virtue of section 14 of the Act, the relevant agencies may not, for the purpose of obtaining communications, private information or equipment data, obtain a property interference authorisation under Part 3 of the 1997 Act if the conduct would (unless done with lawful authority) constitute an offence under the CMA. Where section 14 of the Act applies, the relevant agencies must obtain a targeted equipment interference warrant under Part 5 of the Act to authorise equipment interference, unless the conduct is capable of being authorised under another power (for example if the relevant agencies are exercising any powers of inspection, search or seizure or undertaking any other conduct that is authorised or required under an enactment or rule of law).

2.23 Accordingly, the relevant agencies will apply for a targeted equipment interference warrant under the Act where the CMA is engaged and the conduct cannot be authorised under another power.

2.24 The relevant agencies may only issue a targeted equipment interference warrant if there is a British Islands connection. A British Islands connection exists if:

- any of the conduct authorised by the warrant would take place in the British Islands (regardless of the location of the equipment that would, or may, be interfered with),
- any of the equipment which would, or may, be interfered with would, or may, be in the British Islands at some time while the interference is taking place, or
- a purpose of the interference is to obtain—

i. communications sent by, or to, a person who is, or whom the law enforcement officer believes to be, for the time being in the British Islands,

ii. information relating to an individual who is, or whom the law enforcement officer believes to be, for the time being in the British Islands, or

iii. equipment data which forms part of, or is connected with, communications or information falling within i. or ii above.

2.25 To further ensure that targeted equipment interference activities are focused on investigations or operations within the British Islands the relevant agencies should not obtain a targeted equipment interference warrant for interference that takes place outside of the British Islands unless the subject of investigation is a UK national or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court. For example, such circumstances may arise where material is being acquired from equipment in the British Islands, but the equipment is subsequently temporarily taken outside the British Islands and the material continues to be captured[4].

Example: A relevant agency has obtained an equipment interference warrant authorising the acquisition of communications, information and equipment data from a subject's equipment. The subject temporarily leaves the British Islands with the relevant equipment. The law enforcement agency may continue to obtain material from the equipment while the target is outside the British Islands.

Non-mandatory use of targeted equipment interference warrants

2.26 Section 14 of the Act restricts the ability of relevant agencies to authorise interference with equipment under the 1997 Act. Where the purpose of the interference is to obtain communications, private information or equipment data and the applicant considers the conduct would, unless done with lawful authority, constitute an offence under the CMA, activity which was previously authorised under the 1997 Act should now be authorised under Part 5 of the Act, which is subject to enhanced safeguards tailored for this manner of activity.

2.27 As with existing property interference powers in the 1997 Act, this does not prohibit the relevant agencies from using other powers available to them to access communications, equipment data or other information. In particular, the relevant agencies may continue to exercise their powers of inspection, search or seizure or undertake any other conduct amounting to interference for these purposes that is authorised or required under an enactment or rule of law. For the avoidance of doubt, and notwithstanding any other provisions of this code, an equipment interference warrant will not be required where the interference is authorised under another power.

[4] See section 107 of the Act.

3 Targeted equipment interference warrants

Overview

3.1 Responsibility for issuing targeted equipment interference warrants and the purposes for which warrants may be issued vary depending on the relevant agency applying for the warrant. Targeted equipment interference warrants for Police Scotland and the PIRC are issued by the Chief Constable and the Commissioner, respectively. References to the law enforcement chief are references to the Chief Constable in relation to the Police Service of Scotland and the Commissioner in relation to the Police Investigations and Review Commissioner.

Targeted equipment interference warrants

3.2 A targeted equipment interference warrant described in section 99(2) of the Act authorises or requires the person to whom it is addressed to secure interference with any equipment to obtain communications, equipment data or other information. A warrant may also authorise the disclosure of material obtained under the warrant.

3.3 Except where the law enforcement chief considers that there is an urgent need to issue the warrant, the decision to issue the warrant must be approved by a Judicial Commissioner.

3.4 When targeted equipment interference warrants are issued, the law enforcement chief can address the warrant to the applicant or to another person who is an appropriate law enforcement officer in relation to him. The person to whom the warrant is addressed must be named or described in the warrant. Such a person must be an accountable individual but can be described by their relevant post within the relevant agency. This ensures the law enforcement chief can address the warrant to the most applicable officer who is accountable for giving effect to the warrant.

3.5 Once issued a copy of the warrant may then be served on any person who may be able to provide assistance in giving effect to that warrant.

Subject-matter and scope of targeted warrants

3.6 Section 101 sets out the subject-matter of targeted warrants and constrains what equipment can be described in the warrant; this section therefore sets the “scope” of a targeted warrant. The subject-matter of equipment interference warrants may be targeted or thematic.

Relevant agencies

3.7 Applications for targeted equipment interference warrants may be made by a relevant agency on the grounds of preventing or detecting serious crime. The Police Service of Scotland may also use targeted equipment interference for the purpose of preventing death or injury or any damage to a person’s physical or mental health, or of mitigating any injury or damage to a person’s physical or mental health[5].

[5] Use of equipment interference to prevent death or injury to a person’s physical or mental health or of mitigating any injury or damage to a person’s physical or mental health will only be used in exceptional circumstances. In these circumstances equipment interference techniques will most likely be used to assist in locating vulnerable persons. Accordingly, the Act limits the use of equipment interference for this purpose, making it available to Police Scotland but not the Police Investigations and Review Commissioner. Section 106 of the Act restricts this power to Police Scotland.

3.8 Equipment interference warrants for the relevant agencies must be issued by a law enforcement chief to their relevant law enforcement officer (see section 106 and schedule 6 of the Act, and the Annex of this code).

3.9 The statutory purposes for which equipment interference warrants may be issued reflect the functions of the relevant agency carrying out the equipment interference. Each of the relevant agencies must conduct equipment interference operations in accordance with their statutory or other functions, and the provisions of the Act. So, whilst the Police Investigations and Review Commissioner can issue a warrant where the purpose is the prevention and detection of serious crime, this is limited in that this condition can only be satisfied if the offence, or all of the offences, to which the serious crime relates are being investigated under section 33A(b)(i) of the Police, Public Order and Criminal Justice (Scotland) Act 2006.

Necessity and proportionality

3.10 The Act provides that the person issuing a targeted equipment interference must consider that the warrant is necessary for one or more statutory purposes.

3.11 For all targeted equipment interference warrants the law enforcement chief must also believe that the targeted equipment interference is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that the proposed conduct relates to serious crime may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the material which is sought could reasonably be obtained by other less intrusive means.

3.12 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the interference against what is sought to be achieved;
- explaining how and why the methods to be adopted will minimise the risk of intrusion on the subject and others;
- whether the activity is an appropriate use of the legislation;
- whether there are any implications of the conduct authorised by the warrant for the privacy and security of other users of equipment and systems, including the internet, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation; and
- evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.

3.13 In the case of warrants issued under sections 101(1)(g) and (h) of the Act for the purposes of testing and training, proportionality should be considered by assessing the potential for, and seriousness of, intrusion into any affected person’s privacy against the benefits of carrying out the proposed testing or training exercise.

3.14 It is important that all those involved in undertaking equipment interference activity under the Act are fully aware of the extent and limits of the action that may be taken under the warrant in question.

Targeted warrants relating to a person, organisation or particular location

3.15 In many cases, equipment interference warrants will relate to subjects as set out in section 101(1)(a) and (d). Section 101(1)(a) and (d) warrants are sometimes referred to as "non-thematic" warrants and may relate to one or a combination of:

- equipment belonging to, used by or in the possession of a particular person;
- equipment belonging to, used by or in the possession of a particular organisation; or
- equipment in a particular location.

3.16 A "person" for these purposes may be an individual but, as defined in the Interpretation Act 1978, a person also includes a body of persons corporate or unincorporate. An "organisation" may additionally 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 115(3) will not impose an obligation to name individual employees or workers in the warrant, although the warrant must describe the type of equipment to be interfered with which is likely to include equipment used by those persons. Similarly, in the case of an unincorporated body such as a partnership, a warrant may refer just to the partnership, but will authorise the interference with equipment used by members of that partnership.

3.17 In practice, a relevant agency may need to build intelligence about the legal person or organisation itself, rather than the individuals who are directors, employees or members of 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 risk of collateral intrusion may be higher than a warrant targeting a small subset of individuals working for that organisation. As such, the relevant agency 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. The Act does not require the relevant agency to name or describe individuals within legal persons or organisations in the warrant; in many cases the identities of these individuals will be irrelevant to the intelligence being sought and their identities 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.

3.18 In the case of a particular location, this may relate to interfering with equipment in a building or a defined geographical area where it is not technically feasible to identify individual users of the equipment. Whilst in this instance, activities of individuals may be of intelligence interest, it is the information gained from the equipment described in the warrant in which the relevant agencies are interested.

Format of warrant application

Targeted equipment interference warrants

3.19 An application for a targeted equipment interference warrant should contain the following information:

- a provision stating that it is a targeted equipment interference warrant;
- 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;
- the subject-matter(s) of the warrant, to include the following information dependent on the subject-matter(s):

- equipment belonging to, used by or in the possession of a particular person or organisation must name or describe that person or organisation;
- equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on a particular activity, must name or describe as many of the persons as it is reasonably practicable to name or describe;
- equipment used by or in the possession of more than one person or organisation where the warrant is for the purposes of a single investigation or operation, must describe the nature of the investigation or operation and name or describe as many of the persons or organisations as it is reasonably practicable to name or describe;
- equipment in a particular location must include a description of the location;
- equipment in more than one location where the interference is for the purpose of a single investigation or operation must describe the nature of the investigation or operation and describe as many of the locations as it is reasonably practicable to describe;
- equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description must describe the activity or activities;
- equipment which is being, or may be, used for testing and training purposes must describe the nature of the testing, maintenance or development of capabilities and/or a description of the training.

- a description of any communications, equipment data or other information that is to be (or may be) obtained;
- an outline of how obtaining the material will benefit the investigation or operation. The relevance of the material being sought should be explained along with any considerations which might be relevant to the consideration of the application;
- sufficient information to describe the type of equipment which will be affected by the interference;
- a description of the conduct to be authorised as well as any conduct it is necessary to undertake in order to carry out what is expressly authorised or required by the warrant, including whether communications or other information is to be obtained by surveillance;
- an assessment of the consequences and potential consequences of that conduct, including any risk of compromising the security of any equipment directly or indirectly involved with the interference and, in particular, whether this may enable further intrusion into privacy or impact upon Critical National Infrastructure;
- in the case of thematic warrants, an assessment of whether it will be reasonably practicable to modify the warrant when the identities of the subjects become known and, if so, when such modifications are expected to occur. Where the warrant applicant believes it will not be reasonably practicable to modify the warrant as the identities of individuals, organisations or relevant locations become apparent they should set out the reasons for this.
- the nature and extent of the proposed interference;
- an explanation of why the equipment interference is considered to be necessary on one of the grounds set out in Part 5 of the Act;

- consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, including where appropriate, explaining why less intrusive alternatives have not been or would not be as effective;
- the factors considered when determining if it is proportionate for the warrant to be issued to the appropriate law enforcement officer (see paragraph 3.11);
- what measures will be put in place to ensure proportionality is maintained (for example, the methods by which the material collected will be processed to reduce collateral intrusion (e.g. through filtering or processing the material before any of it is examined), and these can be imposed as conditions on the granting of the warrant);
- consideration of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why that intrusion is justified in the circumstances;
- whether the conduct is likely or intended to result in the obtaining of privileged or other confidential material and, if so, what protections it is proposed will be applied to the handling of the information so obtained;
- where an application is urgent, the supporting justification for that urgency;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results, and an explanation of the collateral intrusion that has arisen to date and how this has been managed;
- an assurance that all material obtained will be kept for no longer than necessary and handled in accordance with the safeguards required by section 129 of the Act and chapter 5 of this code.

3.20 Prior to submission to the person with responsibility for issuing the warrant, each application should be subject to a review within the agency seeking the warrant. This review will consider whether the application is for a purpose specified in the Act and whether the equipment interference proposed is both necessary and proportionate.

Authorisation of targeted equipment interference warrants

3.21 The person responsible for issuing the warrant may only issue a warrant under Part 5 if the person considers that the following tests are met:

The warrant is necessary for the purpose of preventing or detecting serious crime or, in the case of the Police Service of Scotland, for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

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

There are satisfactory safeguards in place. The law enforcement chief must consider that satisfactory arrangements are made for the purposes of the safeguards in section 129 of the Act. These safeguards relate to the copying, dissemination and retention of material obtained by equipment interference and are explained in chapter 5 of this code.

Judicial Commissioner approval. Except in an urgent case, the law enforcement chief may not issue a warrant unless and until the decision to issue the warrant has been approved by a Judicial Commissioner. Section 108 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.

3.22 In addition, the persons responsible for issuing the warrant must consider the general duties in relation to privacy as detailed in section 2 of the Act.

Authorisation of a targeted equipment interference warrant: appropriate delegates

3.23 Where it is not reasonably practicable for a law enforcement chief to issue a warrant an appropriate delegate (listed in Schedule 6 of the Act) may exercise the power to issue the warrant instead in an urgent situation. In these circumstances the appropriate delegate is not signing a warrant on behalf of the relevant law enforcement chief but is issuing the warrant itself. As such, where an appropriate delegate exercises the power to issue a warrant they must follow the same process that would otherwise be followed by a law enforcement chief in an urgent situation.

Authorisation of equipment interference techniques

3.24 Law enforcement chiefs may only issue an equipment interference warrant if they consider that it is proportionate for the warrant to be issued to their appropriate law enforcement officer. In addition to the factors set out in paragraph 3.12 above, in considering whether it is proportionate, the law enforcement chief should consider the full context of the application, including:

- whether the appropriate law enforcement officer, or those effecting the warrant on his behalf, have the capabilities to conduct the equipment interference techniques sought under the warrant;
- whether the equipment interference technique that is sought under the warrant been adequately tested for the proposed use;
- whether the appropriate law enforcement officer, or those effecting the warrant on his behalf, have sufficient training and experience in conducting the equipment interference techniques sought under the warrant;
- if the equipment interference technique is sensitive, whether there are sufficient safeguards in place to ensure that the technique is protected; and
- whether it would be more proportionate for another law enforcement agency to obtain the warrant on their behalf.

Collateral intrusion

3.25 Before authorising applications for targeted equipment interference warrants, the person issuing the warrant should also take into account the risk of obtaining communications, equipment data or other information about persons who are not the targets of the equipment interference activity (collateral intrusion). Particular consideration should be given in cases where collateral intrusion may result in religious, medical, journalistic or legally privileged material being involved, or where communications between a Member of Parliament[6] and another person on constituency business may be involved.

3.26 Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the targeted equipment interference activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the equipment interference activity.

[6] References to a Member of Parliament include references to a member of the House of Commons or the House of Lords, a UK member of the European Parliament, and members of the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

3.27 All warrant applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the person authorising the warrant to fully consider the proportionality of the proposed actions.

Example: A relevant agency seeks to conduct targeted equipment interference against a device used by a subject, T, on the grounds that this is necessary and proportionate for the purpose of preventing or detecting serious crime. It is assessed that the operation will unavoidably result in the obtaining of some information about members of T's family, who are also users of his device, and who are not the intended subjects of the targeted equipment interference. The person issuing the warrant should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation. This may include minimising the obtaining of any material clearly relating to T's family and in the event it is inadvertently captured, applying the safeguards in the Act, including destroying material which is no longer relevant.

3.28 Where it is proposed to conduct targeted equipment interference specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such targeted equipment interference activity should be carefully considered against the necessity and proportionality criteria.

Example: A relevant agency seeks to establish the whereabouts of N. It is proposed to conduct targeted equipment interference against P, who is an associate of N but who is not assessed to be of direct intelligence concern. The targeted equipment interference will enable surveillance to be conducted via P's device, in order to obtain information about N's location. In this situation, P will be the subject of the targeted equipment interference warrant and the person issuing the warrant should consider the necessity and proportionality of conducting surveillance against P, bearing in mind the availability of any other less intrusive means to identify N's whereabouts. It may be the case that the surveillance conducted via P's device will also result in obtaining information about P's family, which in this instance would represent collateral intrusion also to be considered by the person issuing the warrant.

Judicial Commissioner approval

3.29 Before a targeted equipment interference warrant comes into force, its issuance must be approved by a Judicial Commissioner. Section 108 of the Act sets out the test that a Judicial Commissioner must apply when deciding whether to approve the issuance of an equipment interference warrant. This includes reviewing the warrant issuer's conclusion on whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved.

3.30 In reviewing these factors, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review, while ensuring compliance with the general duties in relation to privacy imposed by section 2 of the Act. The Judicial Commissioner may seek clarification of information from the relevant agencies as part of their considerations.

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

- not issue the warrant; or,
- ask the Investigatory Powers Commissioner (IPC) to decide whether to approve or issue the warrant (unless the IPC made the initial decision).

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

3.33 The Act does not mandate how the Judicial Commissioner must show or record their decision. These practical arrangements should be agreed between the relevant agencies and the Investigatory Powers Commissioner. The Act does not, for example, require the Judicial Commissioner to sign a legal instrument. This means that a Judicial Commissioner can provide oral approval to issue a warrant. However, when a Judicial Commissioner refuses to approve a person's decision to issue, they must give the person written reasons. It is important that a written record is taken of any such approvals.

Urgent authorisation of a targeted equipment interference warrant

3.34 The Act makes provision for cases in which a targeted equipment interference warrant is required urgently.

3.35 What constitutes an urgent case is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the requisite time. The requisite time reflects when the authorisation needs to be in place to meet an operational or investigative need. Urgent warrants should fall into at least one of the following three categories:

- imminent threat to life or serious harm. For example, if an individual has been kidnapped and it is assessed that his life is in imminent danger;
- an intelligence gathering opportunity which is significant because of the nature of the potential intelligence, the operational need for the intelligence is significant, or the opportunity to gain the intelligence is rare or fleeting. For example, a group of human traffickers is about to meet to make final preparations to traffic individuals to an unknown location;
- a significant investigative opportunity. For example, a consignment of Class A drugs is about to enter Scotland and Police Scotland wants to have coverage of the perpetrators of serious crime in order to effect arrests.

3.36 The decision by the law enforcement chief to issue an urgent warrant must be reviewed by a Judicial Commissioner within three working days following the day of issue.

3.37 If the Judicial Commissioner retrospectively agrees to the law enforcement chief's or appropriate delegate's issuance of the urgent warrant, and it is still considered necessary and proportionate by the warrant requesting agency, renewal of the urgent warrant may be sought. A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed. If it is renewed it expires after six months, in the same way as non-urgent targeted equipment interference warrants.

Format of equipment interference warrants

3.38 The warrant must describe the type of equipment that is to be interfered with and the conduct that the person to whom the warrant is addressed is authorised to take. The warrant must include the details specified in the second column of the table in section 115 of the Act that relate to relevant equipment described in the first column.

3.39 Each warrant will comprise a warrant instrument signed by the person responsible for issuing the warrant and may also include a schedule or set of schedules. The warrant instrument will include:

- a statement that it is a targeted equipment interference warrant;

- the subject of the equipment interference to which the warrant relates[7]. Where required, descriptions on the instrument can be in the form of an alias or other description that identifies the subject;
- a warrant reference number; and
- the persons who may subsequently modify the warrant in an urgent case (if designated in accordance with section 123 of the Act).

3.40 An equipment interference warrant may expressly authorise the disclosure of any material obtained under the warrant. However, a warrant does not need to specify all potential disclosures of material. Disclosure of material is permitted provided that it is not an unauthorised disclosure for the purposes of section 132 of the Act. This may include, for example, disclosure of material for admission as evidence in criminal and civil proceedings.

Duration of equipment interference warrants

3.41 Targeted equipment interference warrants issued using the standard procedure are valid for an initial period of six months. Warrants issued under the urgency procedure are valid for five working days following the date of issue unless renewed by the law enforcement chief.

3.42 Upon renewal, warrants are valid for a further period of six months. This period begins on the day after the day on which the warrant would have expired, had it 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. An equipment interference warrant may only be renewed in the last 30 days of the period for which it has effect.

3.43 Where a combined equipment interference 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 the periods.

3.44 Where modifications to an equipment interference warrant are made, the warrant expiry date remains unchanged. However, where the modification takes place under the urgency provisions, the modification expires after five working days following the date of issue, unless it is renewed in line with the routine procedure.

3.45 Where a change in circumstance leads the relevant agencies to consider it no longer necessary, proportionate or practicable for a warrant to be in force, the agency must make a recommendation to the law enforcement chief that it should be cancelled with immediate effect.

Failure to approve warrant issued in urgent case

3.46 Where an urgent targeted equipment interference warrant has been issued and the Judicial Commissioner refuses to approve the decision to issue it, the relevant agencies must, as far as reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

3.47 The Judicial Commissioner may:

- authorise further interference with equipment for the purpose of enabling the relevant agencies to secure that anything in the process of being done under the warrant stops as soon as possible;

[7] Eligible subject-matters of equipment interference warrants are set out in section 101.

- direct the destruction of any material obtained under the warrant; and
- impose conditions as to the use or retention of any of that material.

3.48 The Judicial Commissioner may ask the relevant agencies to make representations about how they should exercise their functions in relation to the matters detailed in this paragraph.

Modification of a targeted equipment interference warrant

3.49 Equipment interference warrants may be modified under the provisions of section 123 of the Act. A warrant issued by a law enforcement chief or their appropriate delegate can be modified at any time, by the law enforcement chief or, if the warrant was issued by an appropriate delegate, it can be modified by that person.

3.50 The modifications that may be made are:

- adding to the matters to which the warrant relates;
- removing a matter to which the warrant relates;
- adding any name or description to the names or descriptions included in the warrant. Such a modification cannot be made to a warrant which relates to a targeted subject i.e. that relates to a particular person, organisation or location;
- varying or removing any such name or description. Such a modification cannot be made to a warrant which relates to a targeted subject i.e. that relates to a particular person, organisation or location;
- adding to the descriptions of types of equipment included in the warrant;
- varying or removing a description of a type of equipment included in the warrant.

3.51 The modifications above may be made providing that the conduct authorised by the modification is within the scope of the original warrant. It is for this reason that section 123(3)prohibits modifications to add, vary or remove the name or descriptions of a targeted warrant that relates to just one specified person, organisation or location, as such a modification would go beyond the original scope of the targeted warrant. In practice this means that a warrant which relates to a targeted subject cannot be modified into a targeted thematic warrant; a fresh warrant would be required. Modifications to add names or descriptions, which fall within the scope of the original warrant, are required to be made to targeted thematic warrants when it is reasonably practicable to do so (see paragraph 3.67).

3.52 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:
A relevant agency obtains a targeted equipment interference warrant relating to equipment associated with a specific serious criminal known as 'Mr. Big'. The law enforcement chief, with Judicial Commissioner approval, issues the warrant authorising the interference of equipment of 'Mr. Big'. The investigation progresses and the relevant agency wants to interfere with the equipment of one of 'Mr. Big's' associates. This would require a new warrant – the warrant against 'Mr. Big' cannot be modified so it is against an additional person.

Example of a modification that would be permitted:
A relevant agency obtains a targeted thematic equipment interference warrant relating to equipment associated with a specific serious criminal known as 'Mr. Big' and his unidentified associates. The law enforcement chief, with Judicial Commissioner approval, issues the warrant authorising the interference of equipment of "'Mr. Big' and his unidentified associates investigated

under Operation NAME". The investigation progresses and the relevant agency wants to interfere with the equipment of one of 'Mr. Big's' associates. The warrant could be modified to add the name or description of the associate, if reasonably practicable to do so, and the associate's equipment if it did not fall within the type of equipment already described on the warrant.

3.53 In the case of a modification of a warrant issued to a law enforcement officer, the decision to make a modification must be approved by a Judicial Commissioner, except where the person who made the modification considered that there was an urgent need to make it, (wherein different modification provisions are provided for, detailed below at paragraph 3.54).

Urgent modification of targeted warrants

3.54 Section 123 of the Act makes provision for cases in which modifications of a targeted warrant are required urgently and section 124 provides for the approval process for modifications in urgent cases. A modification 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 kidnapping has taken place, or where intelligence has been received that a significant quantity of drugs is about to enter the country. In some cases, the modification will necessarily be short-lived, for instance if a kidnapping is quickly resolved.

3.55 The relevant law enforcement chief or, if the warrant was issued by an appropriate delegate, an appropriate delegate may make the urgent modification. The modification then must be considered by a Judicial Commissioner within three working days. In the event that the Judicial Commissioner does not agree to the urgent modification, the warrant has effect as if the modification had not been made but the lawfulness of the activity already conducted under the urgent modification is not affected. The person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant, by virtue of the modification, stops as soon as possible. If the Judicial Commissioner refuses to approve the decision to make a modification they may authorise further interference, but only in the interest of ensuring that anything being done by virtue of the modification is stopped as soon as possible.

Renewal of targeted warrants

3.56 Section 117 of the Act sets out that the appropriate person may renew a warrant at any time during the renewal period which is a period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect. Applications for renewals of warrants should contain an update of the matters outlined in paragraph 3.19. In particular, the applicant should give an assessment of the value of equipment interference to date and explain why it is considered that equipment interference continues to be necessary for one or more of the relevant grounds, and why it is considered that the interference continues to be proportionate. Consideration of the extent (if any) of collateral intrusion that has occurred to date, and how this has been managed, will be relevant to the consideration of proportionality. Sections 111 to 114 (additional safeguards) apply in relation to the renewal of warrants in the same way as they apply to a decision to issue a warrant.

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

3.58 A copy of the warrant renewal instrument will be forwarded to all persons on whom a copy of the original warrant has been served, providing they are still actively assisting with the implementation of the warrant. A warrant renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Cancellation of warrants

3.59 Any of the persons authorised to issue warrants under Part 5 of the Act may cancel a warrant at any time. If an appropriate person within the law enforcement agency considers that such a warrant is no longer necessary or that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct, the appropriate person must cancel the warrant. The relevant agencies therefore will need to keep their warrants under review in order to take the appropriate action once the warrant is no longer necessary or proportionate. The relevant agencies should take steps to cease the interference 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.

3.60 The Act requires the person to whom a warrant is addressed to ensure that anything in the process of being done under the warrant stops as soon as possible, so far as is reasonably practicable. In some circumstances it may be impossible, or not reasonably practicable, to cease all elements of interference upon cancellation of a warrant. In deciding what ought to be done to achieve this, a relevant agency must consider what further interference with equipment and privacy might be necessary and whether it is proportionate to undertake it (without further authorisation) in order to stop the original activity. In cases of doubt relevant agencies may seek advice from the IPC.

3.61 The cancellation instrument should be addressed to the person to whom the warrant was issued and should include the reference number of the warrant and the description of the equipment specified in the warrant. A copy of the cancellation instrument should be sent to any persons who have assisted in giving effect to the warrant in the preceding 12 months.

Targeted thematic warrants

3.62 In some cases, Part 5 warrants will relate to subjects linked by a common theme. These are sometimes referred to as targeted “thematic” warrants. Targeted thematic warrants can cover a wide range of activity; it is entirely possible for a thematic warrant to cover a wide geographical area or involve the acquisition of a significant volume of data, provided the strict criteria of the Act are met. Thematic warrants, as set out at section 101 of the Act, may relate to equipment:

a. belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity.

b. belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation.

c. in more than one location, where the interference is for the purpose of a single investigation or operation.

d. which is being, or may be, used for the purposes of a particular activity or activities of a particular description.

e. which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information.

f. which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment.

Specificity of thematic warrants

3.63 The Act requires that certain details must be included in the warrant dependent on the subject-matter(s) of the warrant. For example, a thematic warrant that relates to equipment used by 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. A relevant agency must, when the thematic subject-matter requires it, name or describe as many of the specific persons, organisations, locations or sets of premises as is reasonably practicable at the time of the issue of the warrant. Descriptions of persons, organisations, locations or sets of premises must be as granular as possible, consistent with operational constraints and the information available at the time the warrant is issued.

3.64 Therefore, if known, and if it is reasonably practicable to do so, a relevant agency must name or describe each of the persons, organisations, locations or sets of premises caught by the subject-matter of a thematic warrant when applying for the warrant. In some cases aliases may be used to describe individual subjects where their real name is not yet known.

3.65 However, it may not always be reasonably practicable to include specific names or descriptions. Accordingly there are two types of thematic warrants that vary based upon whether or not it is reasonably practicable to specifically name or describe every subject of the interference.

Example of interference where it is reasonably practicable to include additional details of those falling within the subject-matter of the warrant: A relevant agency wishes to interfere with the equipment of people for the purposes of an investigation into human trafficking. The relevant agency applies for a warrant in relation to "equipment used by more than one person for the purpose of operation X" and three of 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, this warrant authorises interference with the equipment used by ''Mr A', 'Mr B' and 'Mrs C'', the type of equipment must be described within the warrant in accordance with section 115(4). Further equipment or further names must be added by modification (see paragraph 3.71) if the relevant agency wishes to undertake further activity.

Example of interference where it is not reasonably practicable to include additional subject-matter details: A relevant agency wishes to identify persons accessing child pornography material online. The relevant agency seeks a thematic warrant in relation to more than one person carrying on a particular activity, with the subject-matter of the warrant being "equipment used by persons be accessing the child pornography 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 equipment used by persons known to be accessing website 'X' and the authorised interference with any type of equipment described in the warrant falling in to that description is lawful. There is no requirement to modify the warrant in accordance with section 115(3) to add names or descriptions of persons accessing the website.

3.66 In all cases the relevant agencies must have regard to whether what is sought to be achieved by any proposed interference could be achieved by less intrusive means and must seek to provide the issuing authority with individual warrant applications or, if that is not reasonably practicable, a granular list of subjects in a thematic warrant application. Therefore, before submitting a warrant application, the relevant agencies must first consider whether they are able to achieve the intended outcome of an equipment interference operation by seeking non-thematic warrants. If this is not possible an application should be considered for a warrant that specifically names or describes every subject of the interference individually. The relevant agencies must only make an application for a warrant where every subject of the interference is not named or described individually if the preceding options are not reasonably practicable.

3.67 The practicability of providing individual names or descriptions will need to be assessed on a case-by-case basis by the relevant agency making the application and will depend upon, for

example, the existing intelligence picture, the quantity of subjects, the nature of the equipment to be interfered with and the time constraints of the particular operation.

3.68 In some instances it may not be possible to identify individual pieces of equipment or be specific about the nature of the equipment to be interfered with in advance, or there may be a technique that in itself carries out a specific small amount of interference, but enables access to the data that may already have been granted under an existing authorisation. In these cases the warrant should be specific about the technique and the circumstances in which the warrant is to be used. In such cases, the circumstances must be described in a way that enables the requirements of section 115 of the Act to be met.

Authorisation of thematic warrants

3.69 Before issuing a thematic warrant the issuing authority must be satisfied that it is necessary and proportionate to issue it and that the subject-matter is as detailed as is reasonably practicable. In addition, the issuing authority and Judicial Commissioner would have to be satisfied that the method of naming or describing the subjects of the interference was compliant with the requirements of section 115(3) of the Act.

3.70 The information in relation to the names or descriptions to be included in the warrant will assist the issuing authority and Judicial Commissioner in foreseeing the extent of the possible interferences with privacy. The issuing authority'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. This enables the issuing authority and the Judicial Commissioner to be satisfied as to the legality, necessity and proportionality of the proposed conduct. This will also assist those executing the warrant so that they are clear as to the scope of the authorised activity.

Modification of thematic equipment interference warrants

3.71 Thematic equipment interference 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 3.49 to 3.55).

3.72 The modifications that can be made to a thematic equipment interference warrant are:

- adding or removing a matter to which the warrant relates;
- adding, varying or removing a name or description in relation to a subject-matter; or
- adding, varying or removing a description of the type of equipment to be interfered with.

3.73 The ability, and requirement, to modify the names or descriptions included in a targeted equipment interference warrant varies depending on the subject-matter of the original warrant and whether, in the case of thematic warrants, the warrant does or does not specifically name or describe every subject of the interference individually.

3.74 Non-thematic equipment interference warrants (warrants that relate to equipment belonging to, used by or in the possession of a particular person or organisation, or in a particular location) cannot be modified in any way that would alter the conduct authorised by the warrant other than modifying the description of the equipment to be interfered with.

3.75 For thematic equipment interference warrants which do specifically name or describe every subject of the interference individually, modifications must be made to add or remove any names or descriptions. Modifications will also be required where the relevant agency wishes to interfere with a type of equipment that was not originally described in the warrant.

3.76 Where a thematic equipment interference warrant does not specifically name or describe every subject of the interference individually, but instead describes them with a general term, modifications are not required to interfere with the equipment of any person, organisation or equipment in any location if the equipment falls within the description in the warrant.

3.77 Modifications are not necessary in such circumstances as the warrant already provides lawful authority to interfere with the relevant equipment. As described in paragraph 3.69 the issuing authority and Judicial Commissioner must consider this to be necessary and proportionate before issuing the warrant and must clearly understand the extent of the interference that they are authorising. Modifications are also not required where a relevant agency wishes to amend the description of the subject of an equipment interference warrant as long as such an amendment does not alter the conduct that is authorised by that warrant, in accordance with section 99(5) of the Act. However, a modification would be required to add, or remove matters to which the warrant relates or to add, vary or remove a description of a type of equipment.

Renewal of thematic warrants

3.78 The provisions relating to renewal of warrants, described in paragraphs 3.56 – 3.58, apply to thematic warrants. In particular, when seeking to renew a thematic warrant that does not specifically name or describe each subject the applicant should include in the renewal application as much additional information as possible about the known subjects of the warrants and any relevant information about subjects that have not yet been specifically identified. This additional information will ensure that the issuing authority and Judicial Commissioner will have further opportunity to consider the necessity and proportionality of the interference, supported by up-to-date information.

Cancellation of thematic warrants

3.79 There is an ongoing 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 3.59 – 3.61.

3.80 Where persons, organisations and locations are named or described by way of a category rather than individually, there is no ongoing requirement to provide names or descriptions within that category to the issuing authority once the warrant is issued. However, if, over the course of an operation, the relevant agency understands that the description provided and included in the warrant is no longer accurate to the information that they provided in the warrant application they must consider whether the warrant should be cancelled by virtue of the requirement to cancel any warrant that is no longer necessary and proportionate.

Example: A relevant agency may seek a warrant to interfere with the equipment of persons who are users of website 'X', and sets out in the application that they will be unable to individually name or describe the users due to an anticipated large quantity. However, over the course of the operation the relevant agency determines that only a proportion of people falling within description of 'users of website 'X' are of intelligence interest. The relevant agency must assess whether the proportionality case accepted by the issuing authority and Judicial Commissioner remains appropriate. If the change in circumstances affects the proportionality of the warranted activity then the warrant should be modified to reflect more precisely those subject to interference or the issuing authority should be notified that the warrant may need to be cancelled.

Combined warrants

3.81 Where a relevant agency wishes to conduct equipment interference but not all of the proposed conduct can properly be authorised under an equipment interference warrant, additional warrants or authorisations will be required. The relevant agency may either obtain a combined

warrant or may obtain separate warrants/authorisations pursuant to the Act, RIP(S)A or the 1997 Act.

Example: A relevant agency wishes to covertly enter residential premises to search for physical evidence and also download material from a device located within the premises. The obtaining of material from the device constitutes equipment interference. However, the associated entry to property is a separate interference with property and the intrusive surveillance is not linked to the communications, equipment data or other information obtained from the equipment interference. The entry to property and intrusive surveillance cannot be authorised by the equipment interference warrant and must be authorised by a property interference authorisation and intrusive surveillance authorisation respectively (a directed surveillance authorisation may also be required). All three authorisations relate to the same operational activity and the same information will be relevant across the applications. A combined warrant is therefore likely to be appropriate.

3.82 Schedule 8 to the Act provides for combined warrants. Combining warrant applications is not mandatory, but provides the option for grouping warrant applications for the same operational activity together so that the full range of actions that may be undertaken can be addressed. This allows the law enforcement chief and/or Judicial Commissioner to consider the full range of actions that may be undertaken in relation to the investigation. In appropriate cases, it can allow a more informed decision about the necessity and proportionality of the totality of the action to be authorised and can also be more efficient for the relevant agency applying for the warrant.

3.83 In some cases, the decision to combine warrants will necessitate a higher authorisation process than would otherwise be required for individual warrant applications. Where two warrants are combined that would otherwise be issued by different authorities (for example, an equipment interference warrant issued by a law enforcement chief and an interception warrant issued by the Scottish Ministers), the warrant will always be issued by the higher authority level. Where part of a combined warrant is cancelled, the whole warrant ceases to have effect under the same procedures set out at paragraph 3.59.

3.84 Where warrants are sought urgently and the intention is to proceed later with a combined warrant application, such an application must be made before the urgent warrant authorisation ceases to have effect. An urgent warrant authorisation ceases to have effect at the end of the fifth working day after the day on which the warrant was issued.

3.85 As per paragraph 20(1)(a) of Schedule 8, the duties imposed by section 2 (having regard to privacy) apply to combined warrants as appropriate. So the targeted equipment interference element of a combined warrant cannot be issued without having regard to privacy per section 2.

3.86 The exclusion of matters from legal proceedings (section 56) continues to apply to an interception warrant that is part of a combined warrant. However, when an equipment interference warrant is combined with an interception warrant the material derived from equipment interference may still be used in legal proceedings if required. If material derived from equipment interference authorised by a combined warrant can be recognised as a product of interception, and therefore reveals the existence of a warrant issued under Chapter 1 of Part 2 of the Act, the material is excluded from use in legal proceedings according to section 56 of the Act.

3.87 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, the relevant agencies may wish to consider the possibility of seeking individual warrants instead.

Applications made by or on behalf of the relevant agencies

3.88 Paragraph 12 of Schedule 8 sets out that the law enforcement chief of the relevant agencies may issue a warrant that combines a targeted equipment interference warrant with one or more of the following:

- a directed surveillance authorisation under section 6 of RIP(S)A
- an intrusive surveillance authorisation under section 10 of RIP(S)A
- a property interference authorisation under section 93 of the 1997 Act.

Example: A relevant agency wishes to conduct an operation which involves directed surveillance (provided for under section 6 of RIP(S)A) and targeted equipment interference. Under Schedule 8 they may wish to combine these applications. The relevant law enforcement chief would consider the directed surveillance activity as part of the entire combined application. This entire combined application would also require approval by a Judicial Commissioner.

3.89 The above considerations do not preclude relevant agencies from obtaining separate warrants where appropriate. This may be required in order to preserve sensitive techniques, or may be more efficient if other authorisations are already in place.

Example: A relevant agency is monitoring a subject under the authority of a directed surveillance authorisation. An opportunity is identified to conduct equipment interference on the subject's device. It is necessary to continue to monitor the subject to ensure the equipment interference can be conducted covertly and to minimise the risk of compromise. Provided this continued surveillance is authorised under the existing directed surveillance authorisation, a further surveillance authorisation would not be required and therefore a combined warrant is not likely to be appropriate and a separate equipment interference authorisation could be obtained.

Collaborative working

3.90 Any person applying for an equipment interference warrant will need to be aware of particular sensitivities in the local community where the interference is taking place which could impact on the deployment of equipment interference capabilities. The relevant agencies must also take reasonable steps to de-conflict (as relevant) with other agencies (which are able to conduct targeted equipment interference under the Act). Where a warrant applicant considers that conflicts might arise with another agency, they should consult a senior colleague within the other agency.

3.91 In cases where the relevant agencies are acting on behalf of another, the tasking agency should normally obtain the equipment interference warrant. For example, where equipment interference is carried out by the Police Service of Scotland in support of the National Crime Agency (NCA), the warrant would usually be sought by the NCA. Where the operational support of other agencies (in this example, Police Scotland) is foreseen, this should be reflected in the warrant application and specified in the warrant. However, where the relevant agencies consider it would be more proportionate for another agency to obtain the warrant on their behalf, that other agency must obtain the equipment interference warrant. For example, where the Police Service of Scotland considers that there are not sufficient safeguards in place to ensure the protection of a sensitive technique, it may approach the NCA to obtain the warrant.

3.92 Where possible, the relevant agencies should seek to avoid duplication of warrants as part of a single investigation or operation. For example, where two agencies are conducting equipment interference as part of a joint operation, only one warrant is required. Duplication of warrants does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on agencies.

3.93 Where an individual or a non-governmental body is acting under direction of the relevant agencies any activities they conduct which comprise equipment interference for the purposes of the Act definitions, should be considered for authorisation under that Act.

3.94 There are two further important considerations with regard to collaborative working:

- applications for equipment interference warrants by the Police Service of Scotland must only be made by a member or officer of the Police Service of Scotland; and
- applications for equipment interference warrants by the Police Investigations and Review Commissioner must only be made by a member or officer of the Police Investigations and Review Commissioner, regardless of which force or agency is to conduct the activity.

3.95 When collaboration between equipment interference agencies is expected to be required for an operation from the outset the warrant applicant must name each agency in the warrant application. The application should set out why the involvement of each additional agency is required and to what extent they are intended to be involved in the proposed equipment interference. The warrant application should describe specifically the equipment interference that each individual agency is required to conduct.

3.96 Any equipment interference warrant that specifically authorises the activity of multiple equipment interference agencies should specify any relevant restrictions on the sharing of information derived from the interference between such agencies.

3.97 Where the relevant agencies require an international partner – who is not therefore a relevant agency – to undertake an action authorised by a targeted equipment interference warrant, this must be clearly specified within the warrant application. The application must make clear why the assistance of an international partner is required and specify the activity that the relevant agencies intend to request of that partner. Once a warrant is issued, the relevant agencies may work collaboratively with an international partner to carry out equipment interference in accordance with that warrant by virtue of section 126 of the Act.

Incidental conduct

3.98 Where a relevant agency obtains an equipment interference warrant, the warrant also authorises any conduct necessary to undertake what is expressly authorised or required by the warrant (excluding conduct that constitutes the interception of live communications[8]).

3.99 This conduct may therefore include interference with associated or non-target equipment in order to obtain communications, equipment data or other information from the target equipment, providing that the conduct does not constitute live interception.

3.100 When applying for an equipment interference warrant the applicant should set out expressly any foreseeable incidental conduct that will be required to facilitate the equipment interference. It is possible that during the course of equipment interference activity further incidental conduct will be required that was not previously foreseen. This incidental conduct, and the obtaining of any material pursuant to this incidental conduct, is permissible and lawful for all purposes.

Example: A relevant agency has obtained a warrant to acquire communications and other relevant information from a target's device, which it anticipates gaining covert access to for a brief period of time. During the operation, the relevant agency unexpectedly has access to two devices, and cannot determine whether one or both belong to the target. The relevant agency is permitted to

[8] Live communication includes communications in the course of their transmission, but not stored communications.

examine both using equipment interference techniques in order to clarify whether one or both belong to the target – this is incidental conduct, which may involve the obtaining of data from both devices. If one device is then found not to be connected to the target, this will be classed as collateral intrusion and the full equipment interference described in the warrant will not take place against that device and any data already obtained relating to that device will be deleted as soon as possible.

3.101 The warrant applicant, law enforcement chief and Judicial Commissioner should consider the incidental conduct that it may be necessary to undertake in order to do what is authorised on the face of the warrant. In cases where conduct is not clearly incidental, but may instead constitute a separate use of another power, the warrant applicant should consider whether a separate authorisation is required. If the status of incidental conduct remains uncertain the warrant applicant may seek a separate authorisation (a combined authorisation may be appropriate).

Surveillance

3.102 The obtaining of communications or information authorised by a targeted equipment interference warrant includes obtaining those communications or information by surveillance. 'Surveillance' for these purposes includes monitoring, observing or listening to a person's communications or other activities, or recording anything that is monitored, observed or listened to. This could include intrusive surveillance (surveillance carried out in a residence or private vehicle) or directed surveillance (surveillance that is not in an intrusive setting, such as monitoring a subject in a public place).

3.103 A separate authorisation for surveillance under RIP(S)A will not therefore be required providing the conduct comprising the surveillance is properly authorised by a targeted equipment interference warrant. The interference with privacy and property resulting from the targeted equipment interference will be considered as part of the targeted equipment interference authorisation.

3.104 In cases where the relevant agencies wish to obtain communications or information by surveillance under a targeted equipment interference warrant, the proposed activity should be set out in the application and be expressly authorised by the warrant.

3.105 By contrast, where the surveillance is not linked to the communications, equipment data or other information obtained from the equipment interference, this will not be capable of authorisation under a targeted equipment interference warrant.

3.106 For example, if the relevant agencies wish to conduct separate surveillance on the user of a device at the same time as the device itself is being subjected to equipment interference, then this will not be considered as part of the equipment interference authorisation and appropriate surveillance authorisation must be obtained. In this situation a combined warrant may be appropriate (for information on combined warrants, see paragraph 3.81).

Interception

3.107 An equipment interference warrant cannot authorise conduct that would amount to an offence, under section 3(1), of unlawful interception of a communication in the course of its transmission (e.g. live interception of an online video call) except if the warrant authorises the obtaining of a communication stored in or by a telecommunication system. If the Police Service of Scotland wishes to conduct interception of communications other than stored communications, an interception warrant must be obtained under Part 2 of the Act (further guidance on interception warrants may be found in the Interception of Communications Code of Practice).

Trade unions

3.108 The relevant agencies are permitted to apply for a warrant against members or officials of a trade union considered to be a legitimate intelligence target where that is necessary for one or more of the statutory purposes and proportionate to what is sought to be achieved. As set out in section 106(2) of the Act, the fact that the information that would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary for a statutory purpose.

Protection of the privacy and security of other users of equipment and systems, including the internet

3.109 The relevant agencies must not intrude into privacy any more than is necessary to carry out their functions or enable others to do so. To leave targets open to exploitation by others would increase the risk that their privacy would be unnecessarily intruded upon. Targeted equipment interference activity must therefore be carried out in such a way as to appropriately minimise the risk of any increase in the: (i) likelihood or severity of any unauthorised intrusion into the privacy; or (ii) risk to the security of users of equipment or systems (whether or not those equipment or systems are subject to the activities of the relevant agencies).

Example: A relevant agency wishes to obtain communications from a device associated with an intelligence target which is connected to the internet through a network used by a range of individuals, not all of whom are of intelligence interest. Before issuing the warrant, the relevant agency must consider whether the proposed course of action would enable others to intrude into the privacy of users of the network, including those not of intelligence interest as well as the target. If this were to be the case, the relevant agency would (having first determined the necessity and proportionality of the activity proposed) need to be satisfied that the enabling of any such intrusion was minimised to the greatest extent possible.

3.110 In the case of warrants issued for the purposes of testing or training, interference should be carried out in such a way as to appropriately minimise the probability and seriousness of intrusion into the privacy of any persons affected by, or in the vicinity of, the proposed activity.

3.111 Any application for a targeted equipment interference warrant should contain an assessment of any risk to the security or integrity of systems or networks that the proposed activity may involve including the steps taken to appropriately minimise such risk according to paragraph 3.109.

4 Implementation of warrants and communications service provider compliance

4.1 After the decision to issue a warrant has been approved by the Judicial Commissioner it will be forwarded to the person to whom it is addressed – in practice the relevant agency which submitted the application. The relevant agency will carry out the targeted equipment interference itself, and may (in addition to acting on its own) require other persons to provide assistance in giving effect to the warrant.

4.2 Section 128 of the Act permits a number of agencies to serve a warrant on telecommunications operators. This includes the Police Service of Scotland. Before serving the warrant on the telecommunications operators, the Scottish Ministers will be required to approve the steps required for giving effect to the warrant. Approval will be given if the Scottish Ministers consider it to be necessary for the telecommunications operator to take the required steps and the steps are proportionate to what is sought to be achieved.

4.3 Where a copy of an equipment interference warrant has been served on anyone providing a telecommunications service, or who has control of a telecommunications system in the UK, that person is under a duty to take all such steps for giving effect to the warrant as are notified to him or her by or on behalf of the person to whom the warrant is addressed.

4.4 For the purpose of requiring any person to provide such assistance, the relevant agency may serve a copy of the warrant on any person, inside or outside the UK, who is required to provide assistance in relation to that warrant[9].

4.5 Section 127 of the Act provides that service of a copy of a 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:

- 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 for service;
- by making it available for inspection at a place in the UK to the person or to someone acting on the person's behalf (if neither of the above two methods are reasonably practicable). The person to whom the warrant is addressed must take steps to bring the contents of the warrant to the attention of the relevant person.

Provision of reasonable assistance to give effect to a warrant

4.6 Any CSP, or any person who offers or provides a telecommunications service to the UK or has control of a telecommunications system located wholly or partly in the UK, may be required to provide assistance in giving effect to an equipment interference warrant. A warrant can only be served on a person who is considered by the relevant agency to be able to provide the assistance required by the warrant. For the avoidance of doubt, in appropriate circumstances, this does not prevent equipment interference agencies and providers working co-operatively together (without the need for service of a copy of an equipment interference warrant in accordance with section 127).

4.7 In the case of warrants issued to specified law enforcement officers, the Act places a requirement on providers to take all such steps for giving effect to the warrant as were approved by the Scottish Ministers and as are notified to the provider by or on behalf of the law enforcement

[9] See section 127 of the Act.

officer to whom the warrant is addressed (section 128(2)). Section 128(2) and (4) ensures that the steps that providers are required to take are limited to those that the Scottish Ministers have expressly approved as necessary and proportionate to what is sought to be achieved by them. The relevant agencies should endeavour to work co-operatively with persons providing assistance in giving effect to warrants, and should seek to implement warrants on a collaborative basis. Assistance sought will typically comprise (but may not be limited to) the provision of infrastructure by a relevant CSP, or details about the technical specification of relevant equipment.

4.8 When requesting assistance that would involve employees of a telecommunications service provider, the Police Service of Scotland and the Scottish Ministers should consider during the authorisation process:

- what measures should be taken by the relevant agencies to best instruct and support any CSP employees required to assist with implementation; and
- what measures should be taken to minimise any impact upon the CSP and their employees so far as is practicable.

4.9 In some cases the relevant agencies may consider that the same material can be acquired either with assistance of a CSP or independently. The relevant agencies should consider the merits of either approach in the context of the specific operation; this should include the consideration of the criteria in paragraph 3.12.

4.10 The steps which may be required by CSPs are limited to those which it is reasonably practicable to take (section 128 (5)). What is reasonably practicable will be considered on a case-by-case basis, taking into account the individual circumstances of the relevant CSP, and should be agreed after consultation between the CSP and the Scottish Government. Such consultation is likely to include consideration of a number of factors including, but not limited to, the technical feasibility and likely cost of complying with any steps notified to the CSP. As part of the consultation, the CSP may raise any other factor that they consider relevant to whether the taking of such steps is reasonably practicable. The duty is enforceable, for example on application for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or any other appropriate relief.

4.11 Where the relevant agencies require the assistance of a CSP in order to implement a warrant, it must provide one or more of the following to the CSP:

- a copy of the signed and dated warrant with the omission of any schedule contained in the warrant; or
- a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant.

4.12 An optional covering document from the relevant agencies (or the person acting on behalf of the agencies) may also be provided requiring the assistance of the provider and specifying any other details as may be necessary. Contact details with respect to the relevant agencies will either be provided in this covering document or will be available in the handbook provided to all CSPs who maintain a technical capability.

4.13 Section 99(5)(b) of the Act makes lawful any conduct undertaken by a person in pursuance of requirements imposed by or on behalf of a person to whom an equipment interference warrant is addressed. This therefore authorises activity undertaken by CSPs in giving effect to a warrant that would otherwise constitute an offence under the CMA, Data Protection legislation or other relevant legislation. Where assistance is required that - but for section 99(5)(b) - would constitute an offence, the law enforcement chief should consider ways in which the warrant can be executed so as to minimise such activity and the need to rely on section 99(5)(b); this is part of the

consideration of whether the activity authorised by the warrant is proportionate and cannot be achieved by less intrusive means.

5 Handling of information, general safeguards and sensitive professions

Overview

5.1 All material obtained under the authority of a targeted equipment interference warrant must be handled in accordance with safeguards which the law enforcement chief considers to be satisfactory[10]. The details of these safeguards are made available to the IPC, and they must meet the requirements of sections 129 and 130 of the Act which are set out below. Any breach of these safeguards must be reported to the IPC. The relevant 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 relevant agencies must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

5.2 In any case where communications, equipment data or other information are obtained under Part 3 of the 1997 Act, equipment interference agencies must handle the material so obtained in accordance with the safeguards set out in Covert Surveillance and Property Interference Code. Compliance with these safeguards will ensure that the relevant agency handles the material in accordance with safeguards equivalent to those set out in chapter 5 of this code.

Use of material as evidence

5.3 Subject to the provisions in chapter 5 of this code, material obtained through equipment interference may be used as evidence in criminal proceedings. The admissibility of evidence is primarily governed by the common law and impacted by the Human Rights Act 1998.

5.4 Ensuring the continuity and integrity of evidence is critical to every prosecution. When information obtained from equipment interference is used evidentially, the relevant agencies should be able to demonstrate how the evidence has been recovered, and be capable of showing each process through which the evidence was obtained where appropriate to do so.

5.5 Where the product of equipment interference could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

5.6 The relevant agencies are also under a duty to ensure that arrangements are in force to secure: (i) that no information is obtained except so far as necessary for the proper discharge of their functions; and (ii) that no information is disclosed except so far as is necessary for those functions, for the purpose of any criminal proceedings.

General safeguards

5.7 Section 129 of the Act requires that disclosure, copying and retention of material obtained under equipment interference warrants is limited to the minimum necessary for the authorised purposes. Something is necessary for the authorised purposes if the material:

- is, or is likely to become, necessary on any relevant grounds as set out in section 129(7). These are for the purpose of preventing or detecting serious crime, for the prevention of death or injury;
- is necessary for facilitating the carrying out of the functions under the Act of the law enforcement chief or the person to whom the warrant is addressed;

[10] Before issuing a targeted equipment interference warrant a law enforcement chief requires to consider that satisfactory arrangements for safeguards are in force in relation to the warrant: see section 106.

- is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

Reviewing warrants

5.8 Regular reviews of all warrants should be undertaken during their currency to assess the need for the equipment interference activity to continue. The results of a review should be retained for at least three years. Particular attention should be given to the need to review warrants frequently where the equipment interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

5.9 In each case, unless specified by the law enforcement chief or Judicial Commissioner, the frequency of reviews should be determined by the relevant agency which made the application. This should be as frequently as is considered necessary and proportionate.

5.10 In the event that there are any significant and substantive changes to the nature of the interference and/or the identity of the equipment during the currency of the warrant, the relevant agency should consider whether it is necessary to apply for a fresh warrant.

Dissemination of material obtained under an equipment interference warrant

5.11 The number of persons to whom any of the material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. In the same way, only so much of the material may be disclosed as is necessary for the authorised purposes. For example, if a summary of the material will suffice, no more than that should be disclosed.

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

5.13 Section 130 of the Act provides that where material, or a copy of such material, obtained under an equipment interference warrant is handed over to the authorities of a country or territory outside the UK, the law enforcement chief must ensure that arrangements are in force to ensure that the material is only shared if the relevant agency considers that arrangements corresponding to the requirements in section 129 (relating to minimising the extent to which material is disclosed, copied, distributed and retained) will apply to the extent that the law enforcement chief considers appropriate. In particular, the material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed.

Offence of making unauthorised disclosure

5.14 Under section 134 of the Act it is a criminal offence to make an unauthorised disclosure of the existence, content or details relating to an equipment interference warrant, the existence of content of any requirement to provide assistance in giving effect to a warrant, any steps taken in pursuance of a warrant and any material derived from equipment interference. This offence applies to all parties listed in section 132(3). The offence does not apply however if:

- the disclosure is an excepted disclosure according to section 133. For example, a law enforcement officer may be authorised by the person to whom an equipment interference warrant is addressed to disclose material acquired by equipment interference in order to carry out their functions; or
- the individual is unaware that the disclosure of the material in question would be in breach of the duty not to make unauthorised disclosures. This could be because they are not aware that the material they are disclosing is derived from equipment interference, as it may not be identifiable as the product of equipment interference.

5.15 Section 133(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 law enforcement chief 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 129 of the Act and paragraphs 5.11 to 5.13 of this code.

Copying

5.16 The number of copies of material must be limited to the minimum necessary for the authorised purposes. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of an equipment interference warrant, and any record which includes the identities of the persons who owned, used or were in possession of the equipment interfered with under the warrant.

Storage

5.17 Material and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. This requirement to store material securely applies to all those who are responsible for handling it, including providers.

Destruction

5.18 Material and all copies, extracts and summaries which can be identified as the product of an equipment interference warrant, must be marked for deletion and securely destroyed as soon as possible once it is no longer necessary or likely to become necessary for any of the authorised purposes.

5.19 If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid for one or more of the authorised purposes.

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

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

5.21 Where material is obtained by a relevant agency as a result of a request to an international partner to undertake equipment interference on its behalf, the material must be subject to the same internal rules and safeguards that apply to the same categories of material when they are obtained directly by the relevant agencies as a result of equipment interference under the Act.

Material involving confidential journalistic material, confidential personal information and exchanges between a member of a relevant legislature[11] and another person on constituency business

5.22 Particular consideration should be given in cases where material is obtained under a targeted equipment interference warrant and the subject of the obtaining might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information includes where confidential journalistic material may be involved; where equipment interference might involve confidential personal information relating to communications between a medical professional or minister of religion and an individual concerning the latter's health or spiritual welfare; or where material concerning communications between a member of a relevant legislature and another person on constituency business may be involved. In such cases, law enforcement chiefs must have regard to whether the level of protection to be applied in relation to obtaining information by virtue of a warrant is higher because of the particular sensitivity of that information.

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

5.24 Spiritual counselling includes 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.

5.25 Where the intention is to acquire confidential information, a statement to this effect must be contained in the application and the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential personal information is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to whether special handling arrangements are required within the relevant agencies.

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

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

[11] A members of a relevant legislature' means a member of the Scottish Parliament, a member of either House of Parliament, a member of the National Assembly for Wales, a member of the Northern Ireland Assembly, or a member of the European Parliament elected for the United Kingdom.

5.28 Any case where confidential information is retained should be notified to the IPC as soon as reasonably practicable, as agreed with the IPC. Any material which has been retained should be made available to the IPC on request.

Items subject to legal privilege

5.29 In Scotland, items subject to legal privilege means communications between a professional legal adviser and their client, or communications made in connection with, or in contemplation of, legal proceedings and for the purposes of those proceedings which would, by virtue of any rule of law relating to confidentiality of communications, be protected in legal proceedings from disclosure. Legal privilege does not apply to material held with the intention of furthering a criminal purpose. Legally privileged items will lose their protection if, for example, the professional legal adviser is intending to hold or use the items for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

5.30 For the purposes of this code, any communication between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the items do 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 items are subject to legal privilege or over whether the items 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 agencies.

5.31 Section 112 of the Act provides special protections for legally privileged items. Acquiring such items 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 (right to respect for private and family life). The acquisition of items subject to legal privilege (whether deliberately obtained or otherwise) is therefore subject to additional safeguards under this code as set out from paragraph 5.29. The guidance set out may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to other content which has been sought.

5.32 In a case where section 112 applies in relation to making a modification, the warrant must be approved by a Judicial Commissioner.

Legal privilege - Application process for targeted equipment interference warrants

5.33 Where a targeted equipment interference warrant is likely to result in a person acquiring items subject to legal privilege, the application should include, in addition to the reasons why it is considered necessary for the interference to take place, a statement that the applicant considers that the relevant material is likely to include items subject to legal privilege and assessment of how likely it is that items which are subject to legal privilege will be obtained or examined. When the purpose or one of the purposes of the warrant is to obtain privileged items, the application must contain a statement to this effect.

5.34 Where the intention is not to acquire items subject to legal privilege, but it is likely that such items will nevertheless be acquired, that should be made clear in the warrant application and the relevant agency should confirm that any inadvertently obtained items 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 items subject to legal privilege.

5.35 Where the intention is to acquire legally privileged items, the law enforcement chief will only issue the warrant if satisfied that there are exceptional and compelling circumstances that make the authorisation necessary.

5.36 Section 112(6) of the Act provides that there cannot be exceptional and compelling circumstances unless the public interest in obtaining the information outweighs the public interest in the confidentiality of items subject to legal privilege; there are no other means by which the information may be reasonably obtained; and the information is necessary for preventing death or serious injury.

5.37 The law enforcement chief will be able to impose additional conditions such as regular reporting arrangements, so as to be able to exercise his or her discretion on whether a warrant should continue to have effect.

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

Lawyers' material

5.39 Where a lawyer, acting in a professional capacity, is the subject of a targeted equipment interference warrant, it is possible that a substantial proportion of the material which will be obtained will be subject to legal privilege. Therefore, in any case where the subject of a targeted equipment interference warrant is known to be a lawyer acting in a professional capacity where it is intended that a lawyer's material is to be obtained, the relevant agency must assume that section 27 applies.

5.40 The relevant agency will wish to consider which of the three circumstances which apply when items subject to legal privilege will or may be obtained is relevant, and what processes should therefore be followed. In other words, they will need to consider whether items subject to legal privilege are likely to be obtained; whether items subject to legal privilege are intentionally sought; or whether the purpose or one of the purposes is to obtain material that, if it was not created or held 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 items subject to legal privilege and the additional considerations set out at paragraph 5.33 will apply.

5.41 Any such case should also be notified to the IPC during his or her next inspection and any material which has been retained should be made available to the IPC on request.

Handling, retention and deletion

5.42 In addition to safeguards governing the handling and retention of material as provided for in sections 129 of the Act, authorised persons who analyse material obtained by equipment interference should be alert to any communications or items which may be subject to legal privilege. Sections 131 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 destruction.

5.43 A legal adviser in the relevant agency must be consulted when it is believed that material which attracts privilege is obtained. The legal adviser is responsible for determining that material is privileged rather than an officer who is involved in an investigation. In cases where there is doubt as to whether material is privileged or not, the IPC may be informed who will be able to give a view. Where it is discovered that privileged material 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 129(3). If not, the material should not be retained, other than for the purpose of its destruction.

5.44 Material 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 IPC must be notified of the retention of the items as soon as reasonably practicable. Paragraphs 5.45 - 5.47 provide more detail on reporting privileged items to the IPC. Such material 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 129(3). Privileged items must be securely destroyed when their retention is no longer needed for those purposes. If such material 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 IPC

5.45 In those cases where items identified by a legal adviser in the relevant agency as being legally privileged have been acquired, the matter should be reported to the IPC as soon as reasonably practicable.

5.46 Section 131 provides that the IPC must order the destruction of the items or impose conditions on their 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 IPC may still impose conditions as he or she 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 items 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 129(3). In these circumstances, the IPC must impose conditions on the use or retention of the item.

5.47 The IPC 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 for the purpose of preventing death or significant injury. If this condition is met, the IPC may impose conditions as to the use or retention of the items, but the IPC is not obliged to do so. If those conditions are not met, the IPC 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 129(3). The IPC must have regard to any representations made by the relevant agency about the proposed retention of privileged items or conditions that may be imposed.

Dissemination

5.48 In the course of an investigation, a relevant agency will not act on or further disseminate legally privileged items unless it has first informed the IPC that the items have been obtained, 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 before taking action, the relevant agency may take action before informing the IPC. In such cases, the relevant agency should, wherever possible consult a legal adviser. A relevant agency must not disseminate

privileged items if doing so would be contrary to a condition imposed by the IPC in relation to those items.

5.49 The dissemination of legally privileged material 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 132. 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 include all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Office and Procurator Fiscal Service lawyer nor any other prosecuting authority lawyer with conduct of a prosecution should have sight of any legally privileged material, held by the relevant 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 public authority to have sight of or seek to rely on legally privileged material in order to gain a litigation advantage over another party in legal proceedings.

5.50 In order to safeguard against any risk of prejudice or accusation of abuse of process, the relevant agencies must take all reasonable steps to ensure that lawyers or other officials with conduct of legal proceedings should not see legally privileged material 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 relevant agency must seek independent advice from Counsel and, if there is assessed to be a risk that sight of such material could yield a litigation advantage, the direction of the Court must be sought.

Applications to acquire material relating to confidential journalistic material and journalists' sources

5.51 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.

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

- in the case of material contained in a communication, journalistic material which the sender of the communication-
- holds in confidence, or
- intends the recipient, or intended recipient, of the communication to hold in confidence;
- in any other case, journalistic material which a person holds in confidence.

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

5.54 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 nor the source (for example, a news editor who has been sent some notes by a journalist).

5.55 Section 28 sets out the safeguards which apply when a relevant agency applies for a warrant under Part 5 where the purpose, or one of the purposes, of the warrant is to authorise the

acquisition 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 acquisition of material which the relevant agency 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.

5.56 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.

5.57 Section 29 sets out the safeguards which apply when a relevant agency applies for a warrant under Part 5 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 if they consider that appropriate safeguards relating to the handling, retention, use and disclosure of the material are in place.

5.58 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.

5.59 The acquisition of material under part 5 of the Act will 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.

5.60 Where material is created or acquired with the intention of furthering 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. Once material has been broadcast, no confidentiality can attach to the material so it is not confidential journalistic material. 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.

5.61 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 agency and before any further dissemination of the content takes place.

Reporting to the Commissioner

5.62 Where confidential journalistic material, or that which identifies a source of journalistic information, has been obtained and retained, other than for the purposes of destruction - the matter should be reported to the IPC as soon as reasonably practicable.

6 Record-keeping and error reporting

Records

6.1 Records must be available for inspection by the IPC and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, 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 (see section 67(5) of RIPA), 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 equipment interference should be centrally retrievable for at least three years:

- all applications made for warrants and for renewals of warrants;
- the date when a warrant is given;
- whether a warrant is approved under urgency procedures;
- where any application is refused, the grounds for refusal as given by the law enforcement chief or Judicial Commissioner;
- the details of what equipment interference has occurred;
- the result of periodic reviews of the warrants;
- the date of every renewal;
- the date when any instruction was given by the Judicial Commissioner to cease the equipment interference; and
- where relevant, the directions issued by the Judicial Commissioner should they refuse to approve an urgent warrant.

6.2 Records should also be kept of the arrangements by which the requirements of section 129 in relation to minimisation of copying and distribution of material and destruction of material are to be met.

6.3 The relevant agencies should keep the following records:

- all advice provided to the law enforcement chief to support their consideration as to whether to issue or renew the equipment interference warrant; and
- where the issuing of any application is not approved by the Judicial Commissioner, the grounds for refusal as given by the Judicial Commissioner and any associated advice/applications to the IPC if there is an appeal.

6.4 The relevant agencies must also keep a record of the information below to assist the IPC in carrying out his or her statutory functions.

6.5 For the purposes of record-keeping requirements a targeted equipment interference warrant should be taken as referring to a targeted equipment interference warrant issued under part 5 of the Act. In recording this information, each relevant agency must keep a record of the number of:

- applications made by or on behalf of the relevant agencies for a targeted equipment interference warrant;
- applications for a targeted equipment interference warrant that were refused by a law enforcement chief;

- decisions to issue a targeted equipment interference warrant that were refused by a Judicial Commissioner;
- occasions that a referral was made by a law enforcement chief to the IPC, following the decision of a Judicial Commissioner to refuse a targeted equipment interference warrant;
- targeted equipment interference warrants issued by the law enforcement chief and approved by a Judicial Commissioner;
- targeted equipment interference warrants authorised by the law enforcement chief or appropriate delegate;
- targeted equipment interference warrants authorised by the law enforcement chief or appropriate delegate that were subsequently refused by a Judicial Commissioner;
- targeted equipment interference warrants that were renewed by the law enforcement chief and approved by a Judicial Commissioner;
- targeted equipment interference warrants that the Judicial Commissioner refused to approve the renewal of;
- targeted equipment interference warrants that were cancelled; and
- targeted equipment interference warrants extant at the end of the calendar year.

6.6 For each targeted equipment interference warrant issued by the law enforcement chief and approved by a Judicial Commissioner (including warrants issued and approved in urgent cases), the relevant agency 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.

Errors

6.7 This section provides information regarding errors, which are not considered to meet the threshold of a criminal or civil offence.

6.8 A relevant error which must be reported to the IPC is defined in section 231 of the Act and for these purposes includes an error:

- by a relevant agency or other such persons assisting to give effect to a warrant 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; and
- of a description identified for this purpose in a code of practice or in guidance provided by the Commissioner.

6.9 Where an error has occurred but the relevant agency has been acting in good faith, this does not constitute a relevant error on the part of the agency but should still be brought to the attention of the IPC. Situations may arise where an equipment interference warrant has been obtained or modified as a result of the relevant agency having been provided with information relating to equipment – for example, by another domestic intelligence agency, police force or CSP – which later proved to be incorrect, due to an error on the part of the person providing the information, but on which the relevant agency acted in good faith. Whilst these actions do not constitute a relevant error on the part of the relevant agency, such occurrences should be brought to the attention of the Commissioner.

6.10 Proper application of the Act and thorough procedures for operating its provisions, including, for example, the careful preparation and checking of warrants, modifications and schedules, should reduce the scope for making errors.

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

6.12 All errors described in paragraph 6.8 of this code must be reported to the IPC. Errors can have very significant consequences on an affected individual's rights.

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

6.14 An error can only occur after targeted equipment interference has commenced. This section of the code cannot provide an exhaustive list of possible errors. Examples could include:

- targeted equipment interference as described in the Act has, or is believed to, have occurred without valid authorisation;
- targeted equipment interference has taken place that would not have occurred but for conduct or an omission of the part of a member of the relevant agency or CSP;
- human error, such as incorrect transposition of equipment information from an application to a warrant or schedule which leads to the wrong material being acquired;
- warranted targeted equipment interference has taken place on a piece of equipment but the material does not in the event relate to the intended subject where information available at the time of seeking a warrant could reasonably have indicated this;
- a material failure to adhere to the arrangements in force under section 129 of the Act relating to material obtained by targeted equipment interference. For example:
    - over-collection caused by software or hardware errors;
    - unauthorised selection of communications;
    - unauthorised or incorrect disclosure of material; or
    - failure to effect the cancellation of targeted equipment interference.

6.15 When an error has been made, the relevant agency or other person which made the error (e.g. the CSP) must report the error to the IPC as soon as reasonably practicable after it has been established an error has occurred. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full.

6.16 If the relevant agency discovers a CSP error they should inform the IPC and the CSP of the error straight away to enable the CSP to investigate the cause of the error and report it themselves.

6.17 The report sent to IPC in relation to any error must include details of the error, the cause, the amount of material relating to the error obtained or disclosed, any unintended collateral intrusion, any analysis or action taken, whether the material has been retained or destroyed and, a summary of the steps taken to prevent recurrence. Wherever possible, technical systems should incorporate functionality to minimise errors. A senior person within the organisation must undertake a regular review of errors.

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

Serious errors

6.19 Section 231 of the Act states that the IPC must inform a person of any relevant error relating to that person which the IPC considers to be a serious error and that it is in the public interest for the person concerned to be informed of the error.

6.20 The IPC cannot consider an error serious unless the IPC considers the error has caused significant prejudice or harm to the person concerned. In circumstances where a relevant error is deemed to be of a serious nature, the IPC must also decide whether he or she considers that it is in the public interest for the person concerned to be informed of the error. The IPC may therefore investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. 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.

6.21 In making a decision, the IPC must in particular consider:

- the seriousness of the error and its effect on the person concerned; and
- the extent to which disclosing the error would be contrary to the public interest or prejudicial to the prevention or detection of serious crime.

6.22 Before making a decision, the IPC must ask the relevant agency which has made the error to make submissions on the matters above.

7 Oversight

7.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints against public authority use of certain investigatory powers, including those covered by this code. Any complaints about the use of powers as described in this code should be directed to the IPT.

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

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

7.4 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 IPC, who will consider them. In particular, any person who exercises the powers in the Act or described in this code must, in accordance with the procedure set out in chapter 6, report to the IPC 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 relevant public authority. The IPC may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the IPT.

7.5 Should the IPC 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 IPC is under a duty to inform the individual affected. Further information on errors can be found in chapter 6 of this code. The public body which has committed the error will be able to make representations to the IPC before they make their decision on whether it is in the public interest for the individual to be informed. The IPC must also inform the affected individual of their right to apply to the Investigatory Powers Tribunal (see chapter 8 on Complaints 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 IPC must report annually on the findings of their inspections and investigations. This report will be laid before the UK and Scottish Parliaments 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 IPC's report, after consultation with the IPC and the Scottish Ministers (so far as the report relates to functions under Part 3 of the Police Act 1997). If the IPC disagrees with the proposed redactions to his or her report then the IPC may inform the Intelligence and Security Committee of the Westminster Parliament that they disagree with them.

7.6 The IPC 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 publicly available subject to public interest considerations. Relevant agencies and communications service providers may seek general advice from the IPC on any issue which falls within the IPC's statutory remit.

8 Complaints

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

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

8.3 This code does not cover the exercise of the IPT'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: 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
SW1H 9ZQ

8.4 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

Schedule 6: Issue of warrants under section 101 etc to whom this code applies

Part 1

TABLE: PART 1

Law enforcement chiefs	*Appropriate delegates*	*Appropriate law enforcement officers*
The chief constable of the Police Service of Scotland.	Any deputy chief constable or assistant chief constable of the Police Service of Scotland who is designated for the purpose by the chief constable.	A constable of the Police Service of Scotland.

PART 2

TABLE: PART 2

The Police Investigations and Review Commissioner.	A staff officer[12] of the Police Investigations and Review Commissioner who is designated by the Commissioner for the purpose.	A staff officer of the Police Investigations and Review Commissioner.

[12] schedule 6 of the IPA provides that 'staff officer' also includes those members of the Commissioner's staff who have been appointed by the Commissioner.

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

Published by The Scottish Government, July 2017

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA

w w w . g o v . s c o t