Home Office

INTERCEPTION OF COMMUNICATIONS
DRAFT Code of Practice

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

November 2015

Interception of Communications
DRAFT Code of Practice

Presented to Parliament pursuant to section 71(4) of the Regulation of Investigatory Powers Act 2000

November 2015

This publication is available at www.gov.uk/government/publications

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

Print ISBN 9781474124751
Web ISBN 9781474124768

ID 14091502 11/15

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

CONTENTS

1. General

1.1 This code of practice relates to the powers and duties conferred or imposed under Chapter I of Part I of the Regulation of Investigatory Powers Act 2000 ("RIPA"), amended in 2014 by the Data Retention and Investigatory Powers Act 2014 ("DRIPA")[1]. It provides guidance on the procedures that must be followed before interception of communications can take place under those provisions. This code of practice is primarily intended for use by those public authorities listed in section 6(2) of RIPA. It will also allow postal and telecommunication operators and other interested bodies to acquaint themselves with the procedures to be followed by those public authorities.

1.2 RIPA provides that all codes of practice issued under section 71 are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal, or to one of the Commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account.

1.3 This version of the code replaces all previous versions of the code.

[1] The Government has committed to bring forward legislation relating to the security, intelligence and law enforcement agencies' use of investigatory powers and to have that legislation enacted before the sunset provision in the Data Retention and Investigatory Powers Act 2014 takes effect on 31 December 2016.

2. Unlawful interception - criminal and civil offences

2.1 Interception is lawful only in the limited circumstances set out in section 1(5) of RIPA.

2.2 Section 1(1) of RIPA makes it a criminal offence for a person intentionally, and without lawful authority, to intercept in the United Kingdom (UK) any communication in the course of its transmission if that communication is sent via a public postal service or a public telecommunication system. The penalty for unlawful interception is up to two years' imprisonment or a fine up to the statutory maximum.

2.3 Section 1(1A) enables the Interception of Communications Commissioner to serve a monetary penalty notice imposing a fine of up to £50,000 if he or she is satisfied that:

- A person has unlawfully intercepted a communication at a place in the UK;
- The communication was intercepted in the course of its transmission by means of a public telecommunication system;
- The person was not, at the time of the interception, making an attempt to act in accordance with an interception warrant which might explain the interception concerned;
- The person has not committed an offence under section 1(1) of RIPA (intentional unlawful interception).

2.4 Guidance on the administration of these sanctions is available on the Commissioner's website:

http://www.iocco-uk.info

2.5 Section 1(2) of RIPA makes it a crime for a person intentionally and without lawful authority to intercept in the UK any communication in the course of its transmission by means of a private telecommunication system, unless, as set out at section 1(6), the person has a right to control the operation or the use of the system, or has the express or implied consent of such a person to make the interception.

3. General rules on interception with a warrant

3.1 Interception has lawful authority where it takes place in accordance with a warrant issued under section 5 of RIPA. Chapter 9 of this code deals with the circumstances in which interception is permitted without a warrant.

3.2 There are a limited number of persons who can make an application for an interception warrant, or an application can be made on their behalf. These are:

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

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

3.4 All interception warrants are issued by the Secretary of State.[2] Even where the urgency procedure is followed, the Secretary of State personally authorises the warrant, although it is signed by a senior official.

Necessity and proportionality

3.5 Obtaining a warrant under RIPA will only ensure that the interception authorised is a justifiable interference with an individual's rights under Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR) if it is necessary and proportionate for the interception to take place. RIPA recognises this by

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

first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the following statutory grounds:

- In the interests of national security;
- To prevent or detect serious crime;
- To safeguard the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

3.6 These purposes are set out in section 5(3) of RIPA. The Secretary of State must also believe that the interception is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.7 The following elements of proportionality should therefore be considered:

- Balancing the size and scope of the proposed interference against what is sought to be achieved;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods have been considered and were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the addition of the intercept material sought.

Meaning of “telecommunications service”

3.8 Section 2 of RIPA defines “telecommunication service” as any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system. Section 2(8A) of RIPA makes clear that any service which consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a 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. The definition of “telecommunications service” in RIPA is intentionally broad so that it remains relevant for new technologies.

Implementation of warrants

3.9 After a warrant has been issued it will be forwarded to the person to whom it is addressed - in practice the intercepting agency which submitted the application. Section 11 of RIPA then permits the intercepting agency to carry out the interception, or to require the assistance of other persons in giving effect to the warrant. A warrant may be served on any person who is required to provide assistance in relation to that warrant.

3.10 Where a copy of an interception warrant has been served on anyone providing a postal service or a public telecommunications service, or who has control of a telecommunication system in the UK, that person is under a duty to take all such steps for giving effect to the warrant as are notified to him or her by or on behalf of the person to whom the warrant is addressed. This applies to any company offering services to customers in the UK, irrespective of where the company is based. Section 11 also sets out the means by which that duty may be enforced.

3.11 Section 11(2B) of RIPA 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;
- By making it available for inspection at a place in the UK (if neither of the above two methods are reasonably practicable).

Provision of reasonable assistance

3.12 Any person providing a postal service or a public telecommunications service, or who has control of a telecommunications system in the UK, (referred to as communications service providers (CSPs) in this code) may be required to provide assistance in giving effect to an interception warrant. RIPA places a requirement on CSPs to take all such steps for giving effect to the warrant as are notified to them (section 11(4) of RIPA). But the steps which may be required are limited to those which it is reasonably practicable to take (section 11(5)). When considering this test, section 11(5)(a) specifies that regard must be had to any requirements or restrictions under the law of the country where the CSP is based that are relevant to the taking of those steps. It also makes clear the expectation that CSPs will seek to find ways to comply without giving rise to conflict of laws. What is reasonably practicable should be agreed after consultation between the CSP and the Government. If no agreement can be reached it will be for the Secretary of State to decide whether to press forward with civil proceedings. Criminal proceedings may also be instituted by, or with the consent of, the Director of Public Prosecutions.

3.13 Where the intercepting agency requires the assistance of a CSP in order to implement a warrant, it should provide the following to the CSP:

- A copy of the signed and dated warrant instrument;
- The schedule setting out the numbers, addresses or other factors identifying the communications to be intercepted by the CSP for warrants issued in accordance with section 8(1);
- A covering document from the intercepting agency (or the person acting on behalf of the agency) requiring the assistance of the CSP and specifying any other details regarding the means of interception and delivery as may be necessary. Contact details with respect to the intercepting agency will either be provided in this covering document or will be available in the handbook provided to all CSPs who maintain an interception capability.

Provision of interception capability

3.14 Persons who provide a public postal or telecommunications service, or plan to do so, may be required to provide a permanent interception capability (under section 12 of RIPA). The obligations the Secretary of State considers reasonable to impose on such persons to ensure they have a capability are set out in an order made by the Secretary of State and approved by Parliament[3]. Section 12(3A) of RIPA provides for the Secretary of State to serve a notice on a company located outside the UK but providing telecommunications services to customers within the UK, setting out the steps they must take to ensure they can meet these obligations. The Government must seek to consult with the CSP over the content of a notice before it is served.

3.15 Section 12(3B) of RIPA provides that where a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given to the person:

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

3.16 When served with a notice, a CSP, if it feels it unreasonable, may refer that notice to the Technical Advisory Board (TAB) to consider the reasonableness of the technical requirements that are being sought and the financial consequences. Details of how to submit a notice to the TAB will be provided either before or at the time the notice is served.

3.17 Any CSP obliged to maintain a permanent interception capability will be provided with a handbook which will contain the basic information they require to respond to requests for reasonable assistance for the interception of communications.

[3] Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 - http://www.legislation.gov.uk/uksi/2002/1931

Duration of interception warrants

3.18 Interception warrants issued on serious crime grounds are valid for an initial period of three months. Interception warrants issued on national security/economic well-being of the UK grounds are valid for an initial period of six months. A warrant issued under the urgency procedure (on any grounds) is valid for five working days following the date of issue unless renewed by the Secretary of State.

3.19 Upon renewal, warrants issued on serious crime grounds are valid for a further period of three months. Warrants renewed on national security/ economic well-being of the UK grounds are valid for a further period of six months. These dates run from the date on the renewal instrument.

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

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

Stored communications

3.22 Section 2(7) of RIPA defines a communication in the course of its transmission as including any time when the communication is being stored on the communication system in such a way as to enable the intended recipient to collect it or otherwise have access to it. Making the contents of a communication stored in this way available to a person other than the sender or intended recipient therefore constitutes interception. A communication remains in the course of its transmission regardless of whether the communication has previously been read, viewed or listened to. A communication stored in this way remains in the course of its transmission.

3.23 Stored communications may also be accessed by means other than a warrant (see chapter 9). For example, if a communication has been stored on a communication system it may be obtained with lawful authority by means of an existing statutory power such as a production order (under the Police and Criminal Evidence Act 1984[4]) or a search warrant. A production order is an order from a circuit judge[5], who must be satisfied that i) an indictable offence has been committed, ii) the person holds the material and iii) the material requested will be of substantial value to the investigation and iv) it is in the public interest that the material should be produced.

[4] All references to the Police and Criminal Evidence Act 1984 shall be interpreted, insofar as the Code relates to activity in Northern Ireland, as referring to the Police and Criminal Evidence (Northern Ireland) Order 1989.
[5] Or a County court judge in Northern Ireland.

4. Special rules on interception with a warrant

Collateral intrusion

4.1 Consideration should be given to any interference with the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament[6] and another person on constituency business may be involved or communications between a Member of Parliament and a whistle-blower. An application for an interception warrant should state whether the interception is likely to give rise to a degree of collateral infringement of privacy. A person applying for an interception warrant must also consider measures, including the use of automated systems, to reduce the extent of collateral intrusion. Where it is possible to do so, the application should specify those measures. These circumstances and measures will be taken into account by the Secretary of State when considering a warrant application made under section 8(1) of RIPA. Should an interception operation reach the point where individuals other than the subject of the authorisation are identified as investigative targets in their own right, consideration should be given to applying for separate warrants covering those individuals.

Confidential information

4.2 Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. This includes where the communications relate to legally privileged material; where confidential journalistic material may be involved; where interception might involve communications between a medical professional or Minister of Religion and an individual relating to the latter's health or spiritual welfare; or where communications between a Member of Parliament and another person on constituency business may be involved.

4.3 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. See also paragraphs 4.26 and 4.28 - 4.31 for additional safeguards that should be applied in respect of confidential journalistic material.

4.4 The Prime Minister must be consulted in any case where it is necessary to target the communications of a Member of Parliament, apart from those approved by Scottish Ministers, or where it is intended to select for examination an MP's communications intercepted under a section 8(4) warrant.

[6] References to a Member of Parliament include references to a member of the House of Commons, 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.

Communications subject to legal privilege

Introduction

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

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

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

4.8 RIPA does not provide any special protection for legally privileged communications. Nevertheless, intercepting such communications (or selecting them for examination in accordance with section 16 when intercepted under a section 8(4) warrant) is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR as well as engaging Article 8. The interception of communications subject to legal privilege (whether deliberately obtained or otherwise) is therefore subject to additional safeguards under this code as set out at paragraphs 4.9-4.15 below. The guidance set out below may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to other material which has been sought.

Application process for section 8(1) warrants

4.9 Where interception under a section 8(1) warrant is likely to result in a person acquiring communications subject to legal privilege, the application should include, in addition to the reasons why it is considered necessary for the interception to take place, an assessment of how likely it is that communications which are subject to legal privilege will be intercepted. In addition, it should state whether the purpose (or one of the purposes) of the interception is to obtain privileged communications. Where the intention is not to acquire communications subject to legal privilege, but it is likely that such communications will nevertheless be acquired during interception, that should be made clear in the warrant application and the relevant agency should confirm that any inadvertently obtained communications that are subject to legal privilege will be treated in accordance with the

safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to the communications subject to legal privilege.

4.10 Where the intention is to acquire legally privileged communications, the Secretary of State will only issue the warrant under section 8(1) if satisfied that there are exceptional and compelling circumstances that make the authorisation necessary. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb or to national security, and the interception is reasonably regarded as likely to yield intelligence necessary to counter the threat.

4.11 Further, in considering any such application, the Secretary of State must believe that the proposed conduct is proportionate to what is sought to be achieved. In particular the Secretary of State must consider whether the purpose of the proposed interception could be served by obtaining non-privileged information. In such circumstances, the Secretary of State will be able to impose additional conditions such as regular reporting arrangements, so as to be able to exercise his or her discretion on whether a warrant should continue to have effect.

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

Selection for examination of legally privileged section 8(4) material: requirement for prior approval by independent senior official

4.13 Where material intercepted under section 8(4) is to be selected for examination according to a factor that is intended, or is likely to, result in a person acquiring communications subject to legal privilege, the enhanced procedure described at paragraph 4.14 and 4.15 applies.

4.14 An authorised person[7] in a public authority must notify a senior official[8] before using a factor to select any section 8(4) material for examination, where this will, or is likely to, result in the acquisition of legally privileged communications. The notification must address the same considerations as described in paragraph 4.9. The senior official, who must not be a member of the public authority to whom the section 8(4) warrant is addressed, must in any case where the intention is to acquire communications subject to legal privilege, apply the same tests and considerations as described in paragraph 4.10 and 4.11. The authorised person is prohibited from accessing the material until he or she has received approval from the senior official authorising the selection of communications subject to legal privilege.

4.15 In the event that privileged communications are inadvertently and unexpectedly selected for examination (and where the enhanced procedure in paragraph 4.14 has consequently not been followed), any material so obtained must be handled strictly in accordance with the provisions of this chapter. No further privileged communications may be selected for examination by reference to that factor unless approved by the senior official as set out in paragraph 4.14.

[7] See chapter 6.
[8] Senior official is defined in section 81 of RIPA.

Lawyers' communications

4.16 Where a lawyer is the subject of an interception under a section 8(1) warrant or selected for examination in accordance with section 16, it is possible that a substantial proportion of the communications which will be intercepted or selected will be between the lawyer and his or her client(s) and will be subject to legal privilege. Therefore, and for the avoidance of doubt, in any case where a lawyer is the subject of an interception or selection for examination, the application or notification must be made on the basis that it is intended to acquire communications subject to legal privilege and the provisions in paragraphs 4.10, 4.11 and 4.14 will apply, as relevant.

4.17 Any case where a lawyer is the subject of an interception or whose communications have been selected for examination in accordance with section 16 should also be notified to the Interception of Communications Commissioner during his or her next inspection and any material which has been retained should be made available to the Commissioner on request.

Handling, retention and deletion

4.18 In addition to safeguards governing the handling and retention of intercept material as provided for in section 15 of RIPA, officials who examine intercepted communications should be alert to any intercept material which may be subject to legal privilege.

4.19 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 15(4). If not, the material should be securely destroyed as soon as possible.

4.20 Material which has been identified as legally privileged should be clearly marked as subject to legal privilege. 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 15(4). It must be securely destroyed when its 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 remains necessary and proportionate for the authorised statutory purposes.

Dissemination

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

4.22 The dissemination of legally privileged material to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates, including law enforcement authorities. In this regard civil proceedings includes all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Prosecution Service lawyer nor any other prosecuting authority lawyer with conduct of a prosecution should have sight of any communications subject to legal privilege, held by the relevant public authority, 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 communications subject to legal privilege in order to gain a litigation advantage over another party in legal proceedings.

4.23 In order to safeguard against any risk of prejudice or accusation of abuse of process, public authorities must also take all reasonable steps to ensure that (so far as practicable) lawyers or policy officials with conduct of legal proceedings should not see legally privileged communications relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the public authority 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.

Reporting to the Commissioner

4.24 In those cases where communications which include legally privileged communications have been intercepted and retained, the matter should be reported to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any material that is still being retained should be made available to him or her if requested, including detail of whether that material has been disseminated.

4.25 For the avoidance of doubt, the guidance in paragraphs 4.1 to 4.24 takes precedence over any contrary content of an agency's internal advice or guidance.

Communications involving confidential journalistic material, confidential personal information and communications between a Member of Parliament and another person on constituency business

4.26 Particular consideration must also be given to the interception of communications that involve confidential journalistic material, confidential personal information, or communications between a Member of Parliament and another person on constituency business. Confidential journalistic material is explained at paragraph 4.3. 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.

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

4.28 Where the intention is to acquire confidential personal information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential personal information is likely but not

intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to whether special handling arrangements are required within the intercepting agency.

4.29 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 set out in section 15(4). 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.

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

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

4.32 The safeguards set out in paragraphs 4.28 – 4.31 also apply to any section 8(4) material (see chapter 6) which is selected for examination and which constitutes confidential information.

5. Interception warrants (section 8(1))

5.1 This section applies to the interception of communications by means of a warrant complying with section 8(1) of RIPA. This type of warrant may be issued in respect of the interception of communications carried on any postal service or telecommunications system as defined in section 2(1) of RIPA (including a private telecommunications system). Responsibility for the issuing of interception warrants rests with the Secretary of State.

Application for a section 8(1) warrant

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

- Background to the operation in question;
- Person or premises to which the application relates (and how the person or premises feature in the operation);
- Description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the interception operation where this is relevant;[9]
- Description of the conduct to be authorised or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data.[10] This conduct may include the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a);
- An explanation of why the interception is considered to be necessary under the provisions of section 5(3);
- Consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- Consideration of any collateral intrusion and why that intrusion is justified in the circumstances;
- Whether the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, or communications between a Member of Parliament and another person on constituency business;

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

- Where an application is urgent, the supporting justification;
- An assurance that all material intercepted will be handled in accordance with the safeguards required by section 15 of RIPA (see paragraph 7.2).

Authorisation of a section 8(1) warrant

5.3 Before issuing a warrant under section 8(1), the Secretary of State must believe the warrant is necessary:[11]

- In the interests of national security;
- For the purpose of preventing or detecting serious crime; or
- For the purpose of safeguarding the economic well-being of the UK, so far as those interests are also relevant to the interests of national security.

5.4 The Secretary of State will not issue a warrant on section 5(3)(c) grounds if this direct link between the economic well-being of the UK and national security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of the UK which is to be safeguarded is directly related to national security on the facts of the case.

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

Urgent authorisation of a section 8(1) warrant

5.6 RIPA makes provision (section 7(l)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to sign the warrant. In these cases the Secretary of State will still personally authorise the interception but the warrant is signed by a senior official, following discussion of the case between officials and the Secretary of State. RIPA restricts issuing warrants in this way to urgent cases where the Secretary of State has expressly authorised the issue of the warrant (section 7(2)(a)), and requires the warrant to contain a statement to that effect (section 7(4)(a)). A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed by the Secretary of State. If it is renewed it expires after three months in the case of serious crime, or six months in the case of national security or economic well-being, in the same way as other non-urgent section 8(1) warrants.

Format of a section 8(1) warrant

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

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

5.8 The warrant instrument should include:

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

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

- The name of the communication service provider, or the other person who is to take action;
- A warrant reference number; and
- A means of identifying the communications to be intercepted.[12]

Modification of a section 8(1) warrant

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

5.11 Scheduled parts of a warrant may be modified by the Secretary of State, or by a senior official[13] acting upon his or her behalf. A modification to the scheduled part of the warrant may include the addition of a new schedule relating to a CSP on whom a copy of the warrant has not been previously served. Modifications made in this way expire at the same time as the warrant expires. There also exists a duty to modify a warrant by deleting a communication identifier if it is no longer relevant. When a modification is sought to delete a number or other communication identifier, the relevant CSP must be advised and interception suspended before the modification instrument is signed.

5.12 The person to whom the warrant is addressed or a senior official within the same agency may modify the scheduled part of the warrant if the warrant was issued or renewed on national security grounds.[14] Where the warrant specifically authorises it, the scheduled part of the warrant may also be amended in an urgent case by the person to whom the warrant is addressed or a subordinate person (identified in the warrant) within the same agency.[15]

[12] This may include addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying communications (section 8(2) of RIPA).
[13] The official to whom the warrant is addressed, or any of his subordinates, may only modify the scheduled parts of the warrant in the circumstances referred to in paragraph 5.12.
[14] Under section 10(6) and (6A) RIPA.
[15] Under section 10(8) RIPA.

5.13 Modifications of this kind are valid for five working days following the date of issue unless the modification instrument is endorsed within that period by a senior official acting on behalf of the Secretary of State. Where the modification is endorsed in this way, the modification expires upon the expiry date of the warrant.

Renewal of a section 8(1) warrant

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

5.15 Where the Secretary of State is satisfied that the interception continues to meet the requirements of RIPA the Secretary of State may renew the warrant.

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

Warrant cancellation

5.17 The Secretary of State is under a duty to cancel an interception warrant if, at any time before its expiry date, the Secretary of State is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of RIPA. Intercepting agencies will therefore need to keep their warrants under continuous review and must notify the Secretary of State if they assess that the interception is no longer necessary. In practice, the responsibility to cancel a warrant will be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State.

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

Records

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

- All applications made for warrants complying with section 8(1) and applications made for the renewal of such warrants;
- All warrants, and renewals and copies of schedule modifications (if any);

- Where any application is refused, the grounds for refusal as given by the Secretary of State; and
- The dates on which interception started and stopped.

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

5.21 The term ’intercepted material’ is used throughout to include any copy, extract or summary made from the intercepted material which identifies itself as the product of an interception as well as the intercepted material itself.

6. Interception warrants (section 8(4))

6.1 This section applies to the interception of external communications by means of a warrant complying with section 8(4) of RIPA.

6.2 In contrast to section 8(1), a section 8(4) warrant instrument need not name or describe the interception subject or a set of premises in relation to which the interception is to take place. Neither does section 8(4) impose an express limit on the number of external communications which may be intercepted. For example, if the requirements of sections 8(4) and (5) are met, then the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP, could, in principle, be lawfully authorised. This reflects the fact that section 8(4) interception is an intelligence gathering capability, whereas section 8(1) interception is primarily an investigative tool that is used once a particular subject for interception has been identified.

6.3 Responsibility for the issuing of interception warrants under section 8(4) of RIPA rests with the Secretary of State. When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate. The certificate ensures that a selection process is applied to the intercepted material so that only material described in the certificate is made available for human examination. If the intercepted material cannot be selected to be read, looked at or listened to with due regard to proportionality and the terms of the certificate, then it cannot be read, looked at or listened to by anyone.

Section 8(4) interception in practice

6.4 A section 8(4) warrant authorises the interception of external communications. Where a section 8(4) warrant results in the acquisition of large volumes of communications, the intercepting agency will ordinarily apply a filtering process to automatically discard communications that are unlikely to be of intelligence value. Authorised persons within the intercepting agency may then apply search criteria to select communications that are likely to be of intelligence value in accordance with the terms of the Secretary of State's certificate. Before a particular communication may be accessed by an authorised person within the intercepting agency, the person must provide an explanation of why it is necessary for one of the reasons set out in the certificate accompanying the warrant issued by the Secretary of State, and why it is proportionate in the particular circumstances. This process is subject to internal audit and external oversight by the Interception of Communications Commissioner. Where the Secretary of State is satisfied that it is necessary, he or she may authorise the selection of communications of an individual who is known to be in the British Islands. In the absence of such an authorisation, an authorised person must not select such communications.[16]

[16] Section 16(2) of RIPA provides that in the absence of such an authorisation an authorised person must not select communications for examination by factors referable to an individual known to be in the British Islands and with the purpose of identifying material contained in communications sent by or intended for such an individual.

Definition of external communications

6.5 External communications are defined by RIPA to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in the course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. For example, an email from a person in London to a person in Birmingham will be an internal, not external communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because the sender and intended recipient are within the British Islands.

Intercepting non-external communications under section 8(4) warrants

6.6 Section 5(6)(a) of RIPA makes clear that the conduct authorised by a section 8(4) warrant may, in principle, include the interception of communications which are not external communications to the extent this is necessary in order to intercept the external communications to which the warrant relates.

6.7 When conducting interception under a section 8(4) warrant, an intercepting agency must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that are most likely to contain external communications that will meet the descriptions of material certified by the Secretary of State under section 8(4). It must also conduct the interception in ways that limit the collection of non-external communications to the minimum level compatible with the objective of intercepting wanted external communications.

Application for a section 8(4) warrant

6.8 An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. The purpose of such a warrant will typically reflect one or more of the intelligence priorities set by the National Security Council (NSC)[17].

6.9 Prior to submission, each application is subject to a review within the agency making the application. This involves scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 5(3) of RIPA and whether the interception proposed is both necessary and proportionate.

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

- Background to the operation in question:
    - Description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the operation where this is relevant;[18] and

[17] One of the NSC's functions is to set the priorities for intelligence coverage for GCHQ and SIS.
[18] This assessment is normally based upon information provided by the relevant communications service provider.

- Description of the conduct to be authorised, which must be restricted to the interception of external communications, or the conduct (including the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a) of RIPA) it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data.

- The certificate that will regulate examination of intercepted material;
- An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes;
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- Where an application is urgent, supporting justification;
- An assurance that intercepted material will be read, looked at or listened to only so far as it is certified and it meets the conditions of sections 16(2)-16(6) of RIPA; and
- An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of RIPA (see paragraphs 7.2 and 7.10 respectively).

Authorisation of a section 8(4) warrant

6.11 Before issuing a warrant under section 8(4), the Secretary of State must believe the warrant is necessary:

- In the interests of national security;
- For the purpose of preventing or detecting serious crime; or
- For the purpose of safeguarding the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

6.12 The power to issue an interception warrant for the purpose of safeguarding the economic well-being of the UK (as provided for by section 5(3)(c) of RIPA), may only be exercised where it appears to the Secretary of State that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant on section 5(3)(c) grounds if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore identify the circumstances that are relevant to the interests of national security.

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

6.14 When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate in which the Secretary of State certifies that he or she considers examination of the intercepted material to be necessary for one or more of the section 5(3) purposes. The purpose of the statutory certificate is to ensure that a selection process is applied to intercepted material so that only material described in the certificate is made available for human examination. Any certificate must broadly reflect the “Priorities for Intelligence

Collection" set by the NSC for the guidance of the intelligence agencies. For example, a certificate might provide for the examination of material providing intelligence on terrorism (as defined in the Terrorism Act 2000) or on controlled drugs (as defined by the Misuse of Drugs Act 1971). The Interception of Communications Commissioner must review any changes to the descriptions of material specified in a certificate.

6.15 The Secretary of State has a duty to ensure that arrangements are in force for securing that only that material which has been certified as necessary for examination for a section 5(3) purpose, and which meets the conditions set out in section 16(2) to section 16(6) is, in fact, read, looked at or listened to. The Interception of Communications Commissioner is under a duty to review the adequacy of those arrangements.

Urgent authorisation of a section 8(4) warrant

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

6.17 A warrant issued under the urgency procedure lasts for five working days following the date of issue unless renewed by the Secretary of State, in which case it expires after three months in the case of serious crime or six months in the case of national security or economic well-being, in the same way as other section 8(4) warrants.

Format of a section 8(4) warrant

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

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

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

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

6.20 A certificate must be modified by the Secretary of State, except in an urgent case where a certificate may be modified by a senior official provided that the official holds a position in which he or she is expressly authorised by provisions contained in the certificate to modify the certificate on the Secretary of State's behalf, or the Secretary of State has expressly authorised the modification and a statement of that fact is endorsed on the modifying instrument. In the latter case, the modification ceases to have effect after five working days following the date of issue unless it is endorsed by the Secretary of State.

6.21 Where the Secretary of State is satisfied that it is necessary, a certificate may be modified to authorise the selection of communications of an individual in the British Islands.[19] An individual's location should be assessed using all available information. If it is not possible, to determine definitively where the individual is located using that information, an informed assessment should be made, in good faith, as to the individual's location. If an individual is strongly suspected to be in the UK, the arrangements set out in this paragraph will apply.

Renewal of a section 8(4) warrant

6.22 The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 6.10 above. In particular, the applicant must give an assessment of the value of interception to date and explain why it is considered that interception continues to be necessary for one or more of the purposes in section 5(3), and why it is considered that interception continues to be proportionate.

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

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

Warrant cancellation

6.25 The Secretary of State must cancel an interception warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of RIPA. Intercepting agencies will therefore need to keep their warrants under continuous review and must notify the Secretary of State if they assess that the interception is no longer necessary. In practice, the responsibility to cancel a

[19] Section 16(3) of RIPA provides that a certificate may be modified to authorise the selection of communications sent or received outside the British Islands according to a factor (for example name, email address or passport number) which is referable to an individual who is known for the time being to be in the British Islands and where the purpose is the identification of material contained in communications sent by that individual or intended for him.

warrant will be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State.

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

Records

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

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

6.28 Records should also be kept of the arrangements for securing that only material which has been certified for examination for a purpose under section 5(3) and which meets the conditions set out in section 16(2) – 16(6) of RIPA in accordance with section 15 of RIPA is, in fact, read, looked at or listened to. Records should be kept of the arrangements by which the requirements of section 15(2) (minimisation of copying and distribution of intercepted material) and section 15(3) (destruction of intercepted material) are to be met. For further details see the chapter on "Safeguards".

7. Safeguards

7.1 All material intercepted under the authority of a warrant complying with section 8(1) or section 8(4) of RIPA and any related communications data[20] must be handled in accordance with safeguards which the Secretary of State has approved in conformity with the duty imposed on him or her by RIPA. These safeguards are made available to the Interception of Communications Commissioner, and they must meet the requirements of section 15 of RIPA which are set out below. In addition, the safeguards in section 16 of RIPA apply to warrants complying with section 8(4). Any breach of these safeguards must be reported to the Interception of Communications Commissioner. The intercepting agencies must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, the agencies must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

The section 15 safeguards

7.2 Section 15 of RIPA requires that disclosure, copying and retention of intercepted material is limited to the minimum necessary for the authorised purposes. Section 15(4) of RIPA provides that something is necessary for the authorised purposes if the intercepted material:

- Continues to be, or is likely to become, necessary for any of the purposes set out in section 5(3) – namely, in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well-being of the UK[21];
- Is necessary for facilitating the carrying out of the functions of the Secretary of State under Chapter I of Part I of RIPA;
- Is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or the Tribunal;
- Is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of him or her by his or her duty to secure the fairness of the prosecution; or
- Is necessary for the performance of any duty imposed by the Public Record Acts.

[20] References in this code to 'intercepted material' include for the purposes of section 15 any related communications data. Further information regarding the use of related communications data is to be found in the Acquisition and Disclosure of Communications Data Code of Practice.

[21] Intercepted material and related communications data obtained for one purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained for another.

Dissemination of intercepted material

7.3 The number of persons to whom any of the intercepted material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of RIPA. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the intercepted material to carry out those duties. In the same way, only so much of the intercepted material may be disclosed as the recipient needs. For example, if a summary of the intercepted material will suffice, no more than that should be disclosed.

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

7.5 Where intercepted material is disclosed to the authorities of a country or territory outside the UK, the agency must take reasonable steps to ensure that the authorities in question have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary. In particular, the intercepted 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.

Copying

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

Storage

7.7 Intercepted material and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of vetting. This requirement to store intercept product securely applies to all those who are responsible for handling it, including CSPs. The details of what such a requirement will mean in practice for CSPs will be set out in the discussions they have with the Government before a Section 12 Notice is served (see paragraph 3.13).

Destruction

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

7.9 Where an intercepting agency undertakes interception under a section 8(4) warrant and receives unanalysed intercepted material and related communications data from interception under that warrant, the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular intercepting agency on the basis that continued retention of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue.

Personnel security

7.10 All persons who may have access to intercepted material or need to see any reporting in relation to it must be appropriately vetted. On an annual basis, managers must identify any concerns that may lead to the vetting of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed. Where it is necessary for an officer of one agency to disclose intercepted material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

The section 16 safeguards

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

- Ensure that intercepted material is read, looked at or listened to by any person only to the extent that the intercepted material is certified; and
- Regulate the use of selection factors that refer to the communications of individuals known to be currently in the British Islands.

7.12 In addition, any individual selection of intercepted material must be proportionate in the particular circumstances (given section 6(1) of the Human Rights Act 1998).

7.13 The certificate ensures that a selection process is applied to material intercepted under section 8(4) warrants so that only material described in the certificate is made available for human examination (in the sense of being read, looked at or listened to). No official is permitted to gain access to the data other than as permitted by the certificate.

7.14 In general, automated systems must, where technically possible, be used to effect the selection in accordance with section 16(1) of RIPA. As an exception, a certificate may permit intercepted material to be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the material falls within the main categories to be selected under the certificate, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary on the grounds specified in section 5(3) of RIPA. Once those functions have been fulfilled, any copies made of the material for those purposes must be destroyed in accordance with section 15(3) of RIPA. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the Interception of Communications Commissioner during his or her inspections.

7.15 Material gathered under a section 8(4) warrant should be read, looked at or listened to only by authorised persons who receive regular mandatory training regarding the provisions of RIPA and specifically the operation of section 16 and the requirements of necessity and proportionality. These requirements and procedures must be set out in internal guidance provided to all authorised persons and the attention of all authorised persons must be specifically directed to the statutory safeguards. All authorised persons must be appropriately vetted (see paragraph 7.10 for further information).

7.16 Prior to an authorised person being able to read, look at or listen to material, a record[22] should be created setting out why access to the material is required consistent with, and pursuant to, section 16 and the applicable certificate, and why such access is proportionate. Save where the material or automated systems are being checked as described in paragraph 7.14, the record must indicate, by reference to specific factors, the material to which access is being sought and systems should, to the extent possible, prevent access to the material unless such a record has been created. The record should include any circumstances that are likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of the collateral intrusion. All records must be retained for the purposes of subsequent examination or audit.

7.17 Access to the material as described in paragraph 7.15 must be limited to a defined period of time, although access may be renewed. If access is renewed, the record must be updated with the reason for the renewal. Systems must be in place to ensure that if a request for renewal is not made within that period, then no further access will be granted. When access to the material is no longer sought, the reason for this must also be explained in the record.

7.18 Periodic audits should be carried out to ensure that the requirements set out in section 16 of RIPA and Chapter 3 of this code are being met. These audits must include checks to ensure that the records requesting access to material to be read, looked at, or listened to have been correctly compiled, and specifically, that the material requested falls within matters certified by the Secretary of State. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards (as noted in paragraph 7.1) must be reported to the Interception of

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

Communications Commissioner. All intelligence reports generated by the authorised persons must be subject to a quality control audit.

7.19 In order to meet the requirements of RIPA described in paragraph 6.3 above, where a selection factor refers to an individual known to be for the time being in the British Islands, and has as its purpose or one of its purposes, the identification of material contained in communications sent by or intended for him or her, a submission must be made to the Secretary of State, or to a senior official in an urgent case, giving an explanation of why an amendment to the section 8(4) certificate in relation to such an individual is necessary for a purpose falling within section 5(3) of RIPA and is proportionate in relation to any conduct authorised under section 8(4) of RIPA.

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

8. Disclosure to ensure fairness in criminal proceedings

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

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

Exclusion of matters from legal proceedings

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

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

Disclosure to a prosecutor

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

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

8.7 The exception does not mean that intercepted material should be retained against a remote possibility that it might be relevant to future proceedings. The normal expectation is still for the intercepted material to be destroyed in accordance with the general safeguards provided by section 15. The exceptions only come into play if such material

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

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

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

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

Disclosure to a judge

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

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

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

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

9. Interception without a warrant

9.1 Lawful interception can only take place if the conduct has lawful authority (as set out in section 1(5) of RIPA). Section 1(5) of RIPA permits interception without a warrant in the following circumstances:

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

9.2 Interception in accordance with a warrant under section 5 of RIPA is dealt with under chapters 3, 4, 5 and 6 of this code. Interception without lawful authority may be a criminal offence (see paragraph 2.2 of this code).

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

Interception with the consent of both parties

9.4 Section 3(1) of RIPA authorises the interception of a communication if both the person sending the communication and the intended recipient(s) have given their consent.

Interception with the consent of one party

9.5 Section 3(2) of RIPA authorises the interception of a communication if either the sender or intended recipient of the communication has consented to its interception, and directed surveillance by means of that interception has been authorised under Part II of RIPA or authorised under The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA). Further details can be found in chapter 2 of the Covert Surveillance and Property Interference Code of Practice and in chapter 3 of the Covert Human Intelligence Sources Code of Practice[23], or their RIPSA equivalents**.**

Interception for the purposes of a communication service provider

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

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

Lawful business practice

9.7 Section 4(2) of RIPA enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept communications for the purpose of carrying on a business. These regulations apply equally to public authorities. These Lawful Business Practice Regulations can be found on the legislation.gov.uk website:

http://www.legislation.gov.uk/uksi/2000/2699

10. Oversight

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

10.2 The Commissioner carries out biannual inspections of each of the nine interception agencies. The primary objectives of the inspections are to ensure that the Commissioner has the information he or she requires to carry out his or her functions under section 57 of RIPA and produce his or her report under section 58 of RIPA. This may include inspection or consideration of:

- The systems in place for the interception of communications;
- The relevant records kept by the intercepting agency;
- The lawfulness of the interception carried out; and
- Any errors and the systems designed to prevent such errors.

10.3 Any person who exercises the powers in RIPA Part I Chapter I must report to the Commissioner any action that is believed to be contrary to the provisions of RIPA or any inadequate discharge of section 15 safeguards. He or she must also comply with any request made by the Commissioner to provide any such information as the Commissioner requires for the purpose of enabling him or her to discharge his or her functions.

11. Complaints

11.1 RIPA establishes an independent tribunal, the Investigatory Powers Tribunal. The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and determine complaints against public authority use of covert powers and human rights claims against the intelligence agencies. It may decide any case within its jurisdiction.

11.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure are available on the IPT website at: http://www.ipt-uk.com or can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ
0207 035 3711

12. Rules for requesting and handling unanalysed intercepted communications from a foreign government

Application of this chapter

12.1 This chapter applies to those intercepting agencies that undertake interception under a section 8(4) warrant.

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

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

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

12.3 A request falling within the second bullet of paragraph 12.2 may only be made in exceptional circumstances and must be considered and decided upon by the Secretary of State personally.

12.4 For these purposes, a "relevant RIPA interception warrant" means one of the following: (i) a section 8(1) warrant in relation to the subject at issue; (ii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of section 8(4)(b) of RIPA) covering the subject's communications, together with an appropriate section 16(3) modification (for individuals known to be within the British Islands); or (iii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering the subject's communications (for other individuals).

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

12.5 If a request falling within the second bullet of paragraph 12.2 is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intercepting agency according to any factors as are mentioned in section 16(2)(a) and (b) of RIPA unless the Secretary of State has personally considered and approved the examination of those communications by reference to such factors.[24]

12.6 Where intercepted communications content or communications data are obtained by the intercepting agencies as set out in paragraph 12.2, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content[25] and communications data[26] must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.

12.7 All requests in the absence of a relevant RIPA interception warrant to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data) will be notified to the Interception of Communications Commissioner.

[24] All other requests within paragraph 12.2 (whether with or without a relevant RIPA interception warrant) will be made for material to, from or about specific selectors (relating therefore to a specific individual or individuals). In these circumstances the Secretary of State will already therefore have approved the request for the specific individual(s) as set out in paragraphs 12.2.
[25] Whether analysed or unanalysed.
[26] Whether or not those data are associated with the content of communications.

ISBN 978-1-4741-2475-1