Subject: RE: Investigatory Powers Act 2016 [ref:_00Db0K8yP._500b0uXbWb:ref]
From: Customer Contact Centre [redacted]
Date: 17/01/2017 14:59
To: Stop MP lies and Corruption

Dear Mr Jefferson

Thank you for your patience while I have been looking into your query.

I can confirm that the FCA (previously FSA) are named under current legislation the Regulation of Investigatory Powers Act 2000 (RIPA) for the purpose of accessing and acquiring communications data from the UK Communications Service Providers (CSP's).

This is in support of their criminal investigation powers and more latterly in support of our regulatory functions for the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.

For further information you may wish to check the Investigatory Powers Bill - Codes of Practice page on the government website.

I hope this information is helpful.

Yours sincerely

Darren Cotton
Customer Contact Centre
Financial Conduct Authority

Consumer Helpline: 0800 111 6768
Website: www.fca.org.uk
[redacted]

Policy paper

Investigatory Powers Bill: codes of practice

From: Home Office
First published: 1 March 2016
Last updated: 4 October 2016, see all updates
Part of: Investigatory Powers Act

Codes of practice relating to the Investigatory Powers Bill.

Documents

National security notices: draft code of practice

PDF, 444KB, 19 pages

This file may not be suitable for users of assistive technology.
Request an accessible format.

Interception of communications: draft code of practice

PDF, 5.47MB, 106 pages

This file may not be suitable for users of assistive technology.
Request an accessible format.

Security and intelligence agencies' retention and use of bulk personal datasets: draft code of practice

PDF, 824KB, 59 pages

This file may not be suitable for users of assistive technology.
Request an accessible format.

Equipment interference: draft code of practice

PDF, 1.31MB, 97 pages

This file may not be suitable for users of assistive technology.
Request an accessible format.

Communications data: draft code of practice

PDF, 1.01MB, 124 pages

This file may not be suitable for users of assistive technology.
Request an accessible format.

Bulk acquisition: draft code of practice

PDF, 528KB, 51 pages

This file may not be suitable for users of assistive technology.
Request an accessible format.

Detail

To assist Parliament in scrutinising the Investigatory Powers Bill (and at the recommendation of the Joint Committee), the government is publishing drafts of 6 statutory codes of practice that will be made under the act.

These codes of practice address many of the committees' recommendations by providing details of how the powers and obligations will work in practice. The codes will be approved by Parliament and will have statutory force.

Published:

1 March 2016

Updated:

4 October 2016

+ full page history

From:

Home Office

Part of:

Investigatory Powers Act

Benefits

Births, deaths, marriages and care

Business and self-employed

Childcare and parenting

Citizenship and living in the UK

Crime, justice and the law

Disabled people

Driving and transport

Education and learning

Employing people

Environment and countryside

Housing and local services

Money and tax

Passports, travel and living abroad

Visas and immigration

Working, jobs and pensions

How government works

Departments

Worldwide

Policies

Publications

Announcements

Help Cookies Contact Terms and conditions

Rhestr o Wasanaethau Cymraeg Built by the Government Digital Service

Home Office

NATIONAL SECURITY NOTICES
DRAFT Code of Practice

Pursuant to Schedule 7 to the Investigatory Powers Act [ ]

[Autumn] 2016

National Security Notices
DRAFT Code of Practice

Published for consultation alongside the Investigatory Powers Bill

[Autumn] 2016

Contents

1. Introduction

1.1 This Code of Practice relates to the powers and duties conferred or imposed under sections 228, 230, 231, 232 and 233 of Part 9 of the Investigatory Powers Act 2016 ("the Act"). It provides guidance on the procedures to be followed when a national security notice is given. This Code of Practice is intended to set out further detail on the circumstances in which a national security notice can be given; the process that must be followed before a notice can be given; the obligations that are imposed by the service of a notice and the ensuing right of review; and oversight of the use of national security notices.

1.2 The Act provides that all Codes of Practice issued under Schedule 7 are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and capabilities conferred by the Act, it must be taken into account.

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

2. Scope and definitions

What is a national security notice?

2.1 Section 228 of the Act provides that a Secretary of State may give a notice to a telecommunications operator in the UK requiring the taking of such specified steps as are considered necessary in the interests of national security. A notice can be given only if the Secretary of State is satisfied that the steps required are necessary and proportionate. Detail on the definition of a telecommunications operator is provided later in this chapter.

2.2 The power to give a notice under section 228 replaces in part the power that was contained in section 94 of the Telecommunications Act 1984 which has been used for a range of purposes including for civil contingencies and to acquire communications data in bulk. Powers to acquire communications data in bulk are now contained in Chapter 2 of Part 6 of the Investigatory Powers Act. Part 1 of Schedule 9 to the Investigatory Powers Act repeals section 94 of the Telecommunications Act.

2.3 Chapter 3 provides information on the type of support that may be required by a national security notice.

2.4 Section 228 makes clear that a national security notice cannot be used for the primary purpose of interfering with privacy, acquiring communications or data where a warrant or authorisation is available under the Act. In any circumstance where a notice would involve the acquisition of communications or data as its main aim, and an additional warrant or authorisation provided for elsewhere in the Act (or in other legislation such as part two of the Regulation of Investigatory Powers Act 2000 (RIPA), the Intelligence Services Act 1994 (ISA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A)) is available, it would always be required. As such, a notice of itself does not authorise an intrusion into an individual's privacy, where that is the primary purpose. More detail on this is provided in Chapter 3.

What is a telecommunications operator?

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

2.6 Section 237 of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the telecommunication

service provider); and defines 'telecommunications system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the UK or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. The definition of 'telecommunications service' in the Act is intentionally broad so that it remains relevant for new technologies.

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

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

.

3. National Security Notices – general rules

The activity authorised by a notice

3.1 Section 228 of the Act states that a Secretary of State may give a notice to a telecommunications operator in the UK requiring the taking of specified steps as are considered necessary in the interests of national security. A notice can only be given if the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by the conduct.

3.2 The type of support that may be required includes the provision of services or facilities which would help the intelligence agencies in safeguarding the security of their personnel and operations, or in providing assistance with an emergency as defined in section 1 of the Civil Contingencies Act 2004. An emergency is described in that Act as:

a) An event or situation which threatens serious damage to human welfare in the UK

b) An event or situation which threatens serious damage to the environment in the UK

c) War, or terrorism, which threatens serious damage to the security of the UK

3.3 It is not possible to give a list of the full range of the steps that telecommunications operators may be required to take in the interests of national security; not only would this affect the ability of the police and security and intelligence agencies to carry out their work, but as communications technology changes the Secretary of State will need to retain flexibility to respond. However, a notice may typically require a telecommunications operator to provide services to support secure communications by the agencies, for example by arranging for a communication to travel via a particular route in order to improve security. They may additionally cover the confidential provision of services to the agencies within the telecommunications operator, such as by maintaining a pool of trusted staff for management and maintenance of sensitive communications services.

Necessity and proportionality

3.4 The giving of a national security notice can only be justified if the steps it requires are necessary for a legitimate purpose and proportionate to that purpose. The Act recognises this by requiring that the Secretary of State believes that the steps required by the notice are necessary in the interests of national security.

3.5 The Secretary of State must also believe that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the reasonableness of the steps that must be taken

against the need for the activity in protecting national security. Each action authorised should bring an expected benefit and should not be disproportionate or arbitrary.

3.6 A national security notice cannot be used for the primary purpose of interfering with privacy, acquiring communications or data. In any circumstance where a notice would involve the acquisition of communications or data as its main aim, an additional warrant or authorisation provided for elsewhere in the Act (or in RIPA, ISA or RIP(S)A) would always be required. Such authorisation would require an assessment of the necessity and proportionality of the intrusion into privacy. However, there may be very limited circumstances where data might incidentally be acquired through the activity authorised by a national security notice where there isn't a suitable additional warrant or authorisation that could be sought to authorise its acquisition. In those circumstances, the Secretary of State must, in authorising the conduct required in the notice, consider whether it is necessary and proportionate for this data to be acquired incidentally.

3.7 This code does not contain particular provision designed to protect the public interest in the confidentiality of journalistic information and any data which relates to a member of a profession which routinely holds items subject to legal privilege or confidential information, because a notice does not authorise acquiring this information.

Format of national security notice applications

3.8 Responsibility for the issuing of national security notices rests with the Secretary of State. An application to be made to the Secretary of State for a national security notice to be given to a telecommunications operator should contain the following information:

a) The purpose of the notice and what it seeks to achieve;

b) Why it is not possible to achieve the required outcome by using one of the other powers contained in the Investigatory Powers Act;

c) How the activity required by the notice is proportionate to what it seeks to achieve;

d) Whether the activity proposed is likely to interfere with an individual's privacy;

e) An assessment of the reasonableness of the steps the telecommunications operator is required to take, and details of the consultation that has taken place with the telecommunications operator to whom the notice will be given.

3.9 Where the application for a notice identifies that an interference with privacy may occur because personal data may be acquired, the application must make clear that an authorisation to approve the interference with privacy has been obtained. If the interference with privacy is incidental to the national security notice, the application must make that clear and seek the Secretary of State's approval for the interference. The application must therefore:

i. Set out known/expected interference or where there is a potential for interference to occur;

ii. Explain why the interference is necessary and;

iii. Describe any mitigating action which will be taken to keep the interference to a minimum.

3.10 An example of what should be contained in an application for a national security notice is attached at Annex A.

Authorisation of a national security notice

3.11 The Secretary of State may only give a notice under section 228 if the Secretary of State considers the following tests are met:

- **The notice is necessary in the interests of national security;**
- **The conduct authorised by the notice is proportionate to what it seeks to achieve;**
- **Any interference with privacy is authorised** by an appropriate authorisation under the Investigatory Powers Act (or other statute where appropriate) or, where it is incidental and cannot be authorised by other means, it is necessary and proportionate to what the notice seeks to achieve; and
- **There are satisfactory safeguards in place.**

- **Judicial Commissioner approval.** The Secretary of State may not give a notice unless and until the decision to give the notice has been approved by a Judicial Commissioner. Section 230 of the Act sets out that the Judicial Commissioner must review the conclusions that have been reached as to whether the notice is necessary, and whether the conduct that would be authorised is proportionate to what is sought to be achieved.

Duration and Review of National Security Notices

3.12 A national security notice remains in force until it is cancelled. The Secretary of State must keep a notice under review. At six monthly intervals, the Secretary of State must consider whether the activity required by the notice remains necessary and proportionate. As part of the review, the Secretary of State must consider whether any incidental interference with privacy remains necessary and proportionate and should continue to be authorised by the notice and not an alternative authorisation provided for in the Investigatory Powers Act or in other relevant statutes. The review must also consider whether any incidental interference with privacy has occurred since the last review that was not anticipated, and the Secretary of State must be satisfied that any continued interference is justified, and should not be authorised by alternate means.

3.13 The Secretary of State must cancel the notice if the conduct it requires is no longer necessary or proportionate.

4. The giving of a notice and telecommunications operator compliance

4.1 After a notice has been authorised, it is given to the telecommunications operator. Where it is given to anyone providing a telecommunications service, or who has control of a telecommunication system in the UK, that person is under a duty to take all the steps required by the notice. This applies to any company in the UK. Section 231 sets out the means by which that duty may be enforced.

4.2 An example of what a national security notice will look like is contained at Annex B. It is necessarily blank so as not to reveal sensitive capabilities and undermine their effectiveness.

Consultation with operators

4.3 Before giving a notice, the Secretary of State must consult the operator[1]. In practice, consultation is likely to take place long before a notice is given. The Government will engage with an operator who is likely to be subject to a notice in order to provide advice and guidance, and prepare them for the possibility of receiving a notice.

4.4 In the event that the Secretary of State considers it appropriate to give a notice, the Government will take steps to consult the telecommunications operator formally before the notice is given. Should the person to whom the notice is to be given have concerns about the reasonableness, cost or technical feasibility of requirements to be set out in the notice, these should be raised during the consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process.

Matters to be considered by the Secretary of State

4.5 Following the conclusion of consultation with a telecommunications operator, the Secretary of State will decide whether to give a notice. This consideration should include all the aspects of the proposed notice. It is an essential means of ensuring that the notice is justified and that proper processes have been followed.

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

- The likely benefits of the notice – this may take into account projected as well as existing benefits.

[1] See section 231(2).

- The likely number of users of any telecommunications service to which the notice relates, if known.

- The technical feasibility of complying with the notice – taking into account any representations made by the telecommunications operator.

- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the telecommunications operator as part of the notice, such as those relating to security. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money.

- Any other effect of the notice on the telecommunications operator – again taking into account any representations made by the company.

4.7 In addition to the points above, the Secretary of State should consider any other issue which is relevant to the decision.

4.8 The notice must specify the period within which the steps specified in the notice are to be taken. The Secretary of State must consider that period to be reasonable.

Receiving a notice

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

4.10 A person to whom a national security notice is given is under a duty to comply with the notice. The duty to comply with a national security notice is enforceable against a person in the UK by civil proceedings brought by the Secretary of State[2].

Disclosure

4.11 Any person to whom a national security notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence or contents of that notice to any person[3].

[2] See section 231(10)(a).

[3] See section 231(8)

Contribution to the costs of taking the steps required by a national security notice

4.12 Section 225 of the Act recognises that operators incur expenses in complying with requirements in the Act, including steps taken in response to a national security notice. The Act, therefore, allows for appropriate payments to be made in respect of these costs.

4.13 Public funding and support is made available to operators to ensure that they can provide, outside of their normal business practices, the support that is required by a national security notice.

4.14 It is legitimate for an operator to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to take the steps specified by a national security notice.

4.15 This is especially relevant for operators which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke systems.

4.16 Contributions may also be appropriate towards costs incurred by an operator which needs to update its systems to maintain, or make more efficient, the support required by a national security notice. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements specified in the notice.

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

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

Referral of national security notices

4.19 The Act includes clear provisions for the recipient of a notice to request a review of the requirements placed on them in a national security notice should they consider these to be unreasonable. A person may refer the notice back to the Secretary of State for review under section 233 of the Act.

4.20 The circumstances and timeframe within which a telecommunications operator may request a review are set out in regulations made by the Secretary of State and approved by Parliament. Details of how to submit a notice to the Secretary of State for review will be provided either before or at the time the notice is given.

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

4.22 Both bodies must give the relevant telecommunications operator and the Secretary of State the opportunity to provide evidence and make representations to them before reaching their conclusions.

4.23 After considering reports from the TAB and the Judicial Commissioner, the Secretary of State may decide to vary, withdraw or confirm the effect of the notice. Where the Secretary of State's decision is to confirm the effect of the notice, this decision must be approved by the Investigatory Powers Commissioner (IPC). Until this decision is made and approved by the IPC, there is no requirement for the telecommunications operator to comply with those part of the notice that have been referred.

Revocation of national security notices

4.24 A national security notice must be revoked (in whole or in part) if it is no longer necessary to require a telecommunications operator to provide a national security capability as at section 232.

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

4.26 The revocation of a national security notice does not prevent the Secretary of State giving a new notice, covering the same, or different services, to the same operator in the future should it be considered necessary and proportionate to do so[4].

[4] See Section 232(8)

5. Oversight

5.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ('the Commissioner'), whose remit is to provide comprehensive oversight of the use of the powers contained within Part 9 of the Act and adherence to the practices and processes described by this code. By statute the Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work.

5.2 The Investigatory Powers Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. Section 207(3) sets out that the IPC must keep under review the giving and operation of national security notices. The IPC may undertake these inspections, as far as they relate to the IPC's statutory functions, entirely on his or her own initiative or they may be asked to investigate a specific issue by the Prime Minister.

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

5.4 The Commissioner must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the national interest. Only the Prime Minister will be able to authorise redactions to the Commissioner's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

5.5 The Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publically available subject to public interest considerations. Public authorities and telecommunications operators may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce guidance for public

authorities on how to apply and use Investigatory Powers. Wherever possible this guidance will be published in the interests of public transparency.

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

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

Annex A: Detail which must be contained in a national security notice application

National security notice application

An application to the Secretary of State for a national security notice should set out:

- The likely benefits of the notice – this may take into account projected as well as existing benefits.
- The likely number of users of any telecommunications service to which the notice relates, if known.
- The technical feasibility of complying with the notice – taking into account any representations made by the telecommunications operator.
- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the telecommunications operator as part of the notice, such as those relating to security. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money.
- Any other effect of the notice on the telecommunications operator – again taking into account any representations made by the company.

An application should also address the following questions:

Necessity

- **What is the purpose of the notice/ what are you seeking to achieve?** *[Brief description of what the telecommunications operator will be asked to do and why it is necessary in the interest of national security]*
- **Can the same result be achieved using any other statute or other powers in the Investigatory Powers Act?** *[if so, explain why a national security notice is the most appropriate means of achieving the objective]*

Proportionality

- **How is the conduct required by the notice proportionate to what you are seeking to achieve?** *[the application must set out how what the telecommunications operator is being asked to do is proportionate to the objective sought]*

- **Will the activity proposed interfere with an individual's privacy?** *[The application must set out: known/expected interference or where there is a potential for interference to occur; explain why the interference is necessary and; describe any mitigating action which will be taken to keep the interference to a minimum. Where the main purpose is interference with privacy an appropriate authorisation under the Investigatory Powers Act must be sought if one is available. If the interference is incidental or there is no alternative means of authorising, the application must make that clear and seek the Secretary of State's approval for the interference]*

- **Is it reasonable to require the operator to take the steps set out in the notice? Have you consulted the telecommunications operator on whom the notice will be given?** *[The application should highlight any concerns which have been expressed by the intended recipient and describe what action has been/can be taken to mitigate their concerns. The application should also set out the period within which the steps specified in the notice are to be taken and an assessment of why that period is reasonable.]*

- **Is the telecommunications operator on whom the notice is to be given uniquely placed to undertake the activity required by the notice or are other operators subject to similar obligations?**

Annex B: Example of a national security notice

NATIONAL SECURITY NOTICE
UNDER SECTION 228(1) OF THE INVESTIGATORY POWERS ACT [ ]

[Insert telecommunications operator's name]

1. In exercise of the power conferred by section 228 of the Investigatory Powers [Act 2016] the Secretary of State considers that it is necessary to require *[insert telecommunications operator's name]* to take the steps set out in this notice. A Judicial Commissioner has approved the Secretary of State's decision.

2. The requirements set out in paragraph 5 of this notice are necessary in the interests of national security and proportionate to what is being sought to be achieved.

3. *[insert telecommunications operator's name]* must :

   a. **[Having appropriate systems in place to carry out the task required]**

   b. **[Issuing instructions to staff which achieve the requirements set out in article 3]**

4. The requirements and results referred to in paragraph 2 are:

   a. **[List the specific tasks which the operator is required to undertake in support of the notice]**

   b.

   c.

5. The steps set out in paragraph 5 must be taken by [date].

6. [insert other information as necessary relating to the operation of the direction].

7. Insert one of the following statements:
   a. no private/personal data will be acquired as a result of the activity required by this notice

b. any private/personal data acquired as a result of the activity required by this notice has been authorised under *[insert as required] or*
c. any private/personal data acquired as a result of the activity required by this notice is incidental and hereby authorised

8. The direction(s) given to *[insert telecommunications operator's name]* by the Secretary of State under section 94 of the Telecommunications Act 1984

Or

The notice given to [*insert telecommunications operator's name]* under section 228 of the Investigatory Powers Act [ ]

is revoked.

In accordance with section 233 of the Investigatory Powers Act [ ], *[insert telecommunications operator's name]* may seek a review of this notice

Signed……..
Her Majesty's Secretary of State for [the Home Department]
Dated

Home Office

Interception of Communications

Pursuant to Schedule 7 to the Investigatory Powers Act

[Autumn 2016]

DRAFT Code of Practice

Contents

1. Introduction

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

1.2. The Act provides that all codes of practice issued under Schedule 7 are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and capabilities conferred by the Act on the intercepting agencies, it must be taken into account.

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

2. Scope and definitions

What is interception?

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

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

What is a communications service provider?

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

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

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

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

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

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

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

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

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

What is meant by the content of a communication?

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

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

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

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

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

Postal definitions

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

What is meant by postal data?

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

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

3. Unlawful interception – criminal and civil offences

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

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

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

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

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

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

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

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

4. Warranted interception – general rules

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

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

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

Types of interception warrant

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

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

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

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

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

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

Necessity and proportionality

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

- In the interests of national security;

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

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

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

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

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

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

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

4.9 The following elements of proportionality should therefore be considered:

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

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

Trade Unions

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

The intercepting authorities

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

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

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

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

- The Director General of the Security Service.

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

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

5. Targeted interception warrants

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

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

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

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

Reviewing warrants

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

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

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

Format of warrant applications

Targeted interception warrants

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Targeted examination warrants

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

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

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

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

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

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

e)

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

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

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

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

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

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

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

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

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

Mutual Assistance Warrants

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

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

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

Subject-matter and scope of targeted warrants

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

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

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

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

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

Example 1

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

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

Targeted thematic warrants

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

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

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

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

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

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

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

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

Example 1

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

Example 2

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

Example 3

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

Example 4

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

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

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

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

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

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

Combined warrants

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

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

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

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

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

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

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

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

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

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

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

Applications made by or on behalf of the intelligence services

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

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

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

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

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

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

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

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

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

- A targeted equipment interference warrant under section 100

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

Applications issued by Scottish Ministers

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

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

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

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

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

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

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

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

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

Format of warrant instruments and schedules

Targeted interception warrants

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

5.45 The warrant instrument will include:

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

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

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

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

[7] See section 235 of the Act.

Targeted examination warrants

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

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

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

Mutual assistance warrants

5.49 Each mutual assistance warrant will include:

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

[8] See section 235 of the Act.

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

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

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

- Whichever of the following statements is applicable:

Either:

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

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

Authorisation of a targeted warrant

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

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

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

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

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

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

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

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

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

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

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

- not issue the warrant;

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

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

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

Power of Scottish Ministers to issue warrants

5.55 Interception warrants may be issued on "serious crime" grounds by Scottish ministers, by virtue of arrangements under the Scotland Act 1998. In this code references to the "Secretary of State" should be read as including Scottish ministers where appropriate. The functions of the Scottish ministers also cover renewal, modification and cancellation arrangements. Sections21 and 22 of the Act make provision for Scottish Ministers to issue targeted interception warrants for serious crime purposes in certain circumstances. Scottish Ministers may issue a targeted interception warrant, a targeted examination warrant or for serious crime purposes providing the warrant, if issued, would relate to a person or group of persons in Scotland or premises which are in Scotland. They may also issue a mutual assistance warrant if it would relate to a person or group of persons, or to premises in Scotland.

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

Per section 21(3):

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

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

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

Per section 21(4):

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

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

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

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

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

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

Judicial commissioner approval

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

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

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

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

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

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

Urgent authorisation of a targeted interception warrant

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

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

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

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

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

Warrants ceasing to have effect

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

5.68 The diagram at Annex A illustrates the authorisation process.

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

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

Duration of interception warrants

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

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

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

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

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

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

Modification of targeted warrants

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

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

Major Modifications

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

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

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

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

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

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

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

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

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

Minor modifications

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

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

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

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

5.81 A minor modification may require a new schedule to be issued to a communications service provider on whom a copy of the warrant has not been previously served. Modifications made in this way will expire at the same time as the warrant expires. There also exists a duty[15] to modify a warrant by deleting a communication identifier if it is no longer relevant. When a modification is sought to delete a number or other communication identifier, the relevant communications service provider must be advised and interception suspended before the modification instrument is signed.

Administrative clarifications of targeted warrants

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

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

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

[15] 34(10)

Urgent major modification of targeted warrants

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

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

Renewal of targeted interception warrants

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

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

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

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

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

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

Warrant cancellation

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

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

6. Bulk interception warrants

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

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

6.3 Bulk interception may be used, for example:

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

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

Bulk interception in practice

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

Bulk Interception

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

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

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

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

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

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

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

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

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

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

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

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

Application for a bulk interception warrant

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

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

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

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

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

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

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

Format of a bulk interception warrant

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

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

Additional requirements in respect of warrants affecting overseas operators

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

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

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

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

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

Authorisation of a bulk interception warrant

Necessity

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

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

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

Proportionality

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

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

Safeguards

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

Judicial Commissioner Approval

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

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

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

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

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

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

Modification of a bulk interception warrant

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

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

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

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

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

Urgent modifications of a bulk interception warrant

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

6.41 In these cases a statement of that fact must be endorsed on the modifying instrument, and the modification ceases to have effect after five working days following the date of issue unless it is approved by a Judicial Commissioner. If a Judicial Commissioner refuses to approve the modification, the modification will cease. Any material collected between the modification being made and the Judicial Commissioner reviewing and refusing the modification will be lawful.

Renewal of a bulk interception warrant

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

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

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

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

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

Warrant cancellation

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.64 Access to the content as described in paragraph 6.63 must be limited to a defined period of time, although access may be renewed. If access is renewed, the record must be updated with the reason for the renewal. Systems must be in place to ensure that if a request for renewal is not made within that period, then no further access will be granted.

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

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

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

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

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

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

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

7. Implementation of warrants and communications service provider compliance

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

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

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

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

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

Provision of reasonable assistance to give effect to a warrant

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

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

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

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

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

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

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

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

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

Duty not to disclose the existence of a warrant

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

Contribution to costs for giving effect to an interception warrant

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

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

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

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

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

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

8. Maintenance of a technical capability

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

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

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

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

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

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

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

Consultation with service providers

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

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

Matters to be considered by the Secretary of State

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

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

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

[19] See section 231(2).

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

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

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

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

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

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

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

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

Giving a notice

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

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

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

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

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

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

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

[20] See section 231 (6).

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

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

Disclosure of technical capability notices

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

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

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

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

Regular review

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

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

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

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

[23] See section 231(8)

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

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

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

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

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

Variation of technical capability notices

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

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

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

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

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

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

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

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

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

Revocation of technical capability notices

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

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

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

Referral of technical capability notices

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

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

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

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

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

Contribution of costs for the maintenance of a technical capability

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

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

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

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

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

General considerations on appropriate contributions

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

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

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

Power to develop compliance systems

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

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

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

Security, integrity and disposal of interception capabilities

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

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

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

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

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

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

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

Security

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

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

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

- Procedural security e.g. processes and controls.

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

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

Integrity of interception and delivered product

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

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

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

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

Principles of data security, integrity and disposal of systems

Legal and regulatory compliance

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

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

Information security policy & risk management

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

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

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

Human Resources Security

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

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

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

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

Maintenance of Physical Security

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

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

Operations management

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

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

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

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

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

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

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

Access Controls

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

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

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

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

Management of incidents

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

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

Additional requirements relating to the disposal of systems

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

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

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

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

9. Safeguards (including sensitive professions)

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

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

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

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

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

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

Dissemination of intercepted content

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

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

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

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

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

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

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

Copying

9.10 Intercepted content may only be copied to the extent necessary for the authorised purposes set out in sections 51(3) and 140(3) of the Act. Copies include not only direct copies of the whole of the intercepted content, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which includes the identities of the persons to or by whom the intercepted content was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.

Storage

9.11 Intercepted content and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of vetting. This requirement to store intercept product securely applies to all those who are responsible for handling it, including communications service providers. The details of what such a requirement will mean in practice for communications service providers will be set out in the discussions they have with the Government before being asked to give effect to a warrant.

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

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

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

Destruction

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

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

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

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

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

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

Application of this chapter

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

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

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

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

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

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

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

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

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

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

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

[28] Whether analysed or unanalysed.

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

Collateral intrusion

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

Confidential information and sensitive professions

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

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

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

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

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

9.31 Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, where the content in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence, or is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

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

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

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

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

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

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

Communications subject to legal privilege

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

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

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

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

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

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

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

Example

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

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

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

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

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

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

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

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

Lawyers' communications

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

[30] Senior official is defined in section 145

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

Handling, retention and deletion

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

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

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

Dissemination

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

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

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

Reporting to the Commissioner

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

10. Record keeping and error reporting

Records

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

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

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

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

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

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

Targeted Warrants

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

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

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

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

Bulk Interception Warrants

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

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

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

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

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

Errors

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Serious errors

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

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

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

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

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

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

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

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

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

11. Disclosure to ensure fairness in proceedings

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

11.2 This part of the code applies to the handling of intercepted content in the context of criminal proceedings where the content has been retained for one of the purposes authorised in section 51(3) of the Act. For those who would ordinarily have had responsibility under the Criminal Procedure and Investigations Act 1996 to provide disclosure in criminal proceedings, this includes those rare situations where destruction of intercepted content has not taken place in accordance with section 51(5) and where that content is still in existence after the commencement of a criminal prosecution. In these circumstances, retention will have been considered necessary to ensure that a person conducting a criminal prosecution has the information he or she needs to discharge his or her duty of ensuring its fairness (section 51(3)(d)).

Exclusion of matters from legal proceedings

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

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

Disclosure to a prosecutor

11.5 Paragraph 21(1)(a) of Schedule 3 provides that intercepted content obtained by means of a warrant and which continues to be available may, for a strictly limited purpose, be disclosed to a person conducting a criminal prosecution.

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

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

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

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

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

Disclosure to a judge

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

11.12 This access will be achieved by the prosecutor inviting the judge to make an order for disclosure to him or her alone, under this subparagraph. This is an exceptional procedure; normally, the prosecutor's functions under paragraph 21(1)(a), will not fall to be reviewed by the judge. To comply with section 53(1), any consideration given to, or exercise of, this power must be carried out without notice to the defence. The purpose of this power is to ensure that the trial is conducted fairly.

11.13 The judge may, having considered the intercepted content disclosed to him or her, direct the prosecution to make an admission of fact. The admission will be abstracted from the interception; but, in accordance with the requirements of section 53(1), it must not reveal the fact of interception. This is likely to be a very unusual step. The Act only allows it where the judge considers it essential in the interests of justice.

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

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

Disclosure to ensure thorough investigations in inquests and inquiries

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

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

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

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

12. Other lawful authority to undertake interception

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

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

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

12.3 The general rule is that neither the possibility of interception, nor intercepted content itself, plays any part in legal proceedings. This rule is set out in section 53 of the Act, which excludes evidence, questioning, assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under this Act.

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

Interception with the consent of one or both parties

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

12.6 Section 42(2) of the Act authorises the interception of a communication if either the sender or intended recipient of the communication has consented to its interception, and directed surveillance by means of that interception has been authorised under Part 2 of RIPA or he Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA). Further details can be found in chapter 2 of the Covert Surveillance and Property Interference Code of Practice and in chapter 3 of the Covert Human Intelligence Sources Code of Practice[34], or their RIPSA equivalents.

Interception by providers of postal or telecommunications services

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

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

Interception by businesses for monitoring and record-keeping purposes

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

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

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

Interception in accordance with overseas requests

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

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

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

Stored communications

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

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

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

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

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

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

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

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

13. Oversight

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

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

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

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

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

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

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

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

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

14. Complaints

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

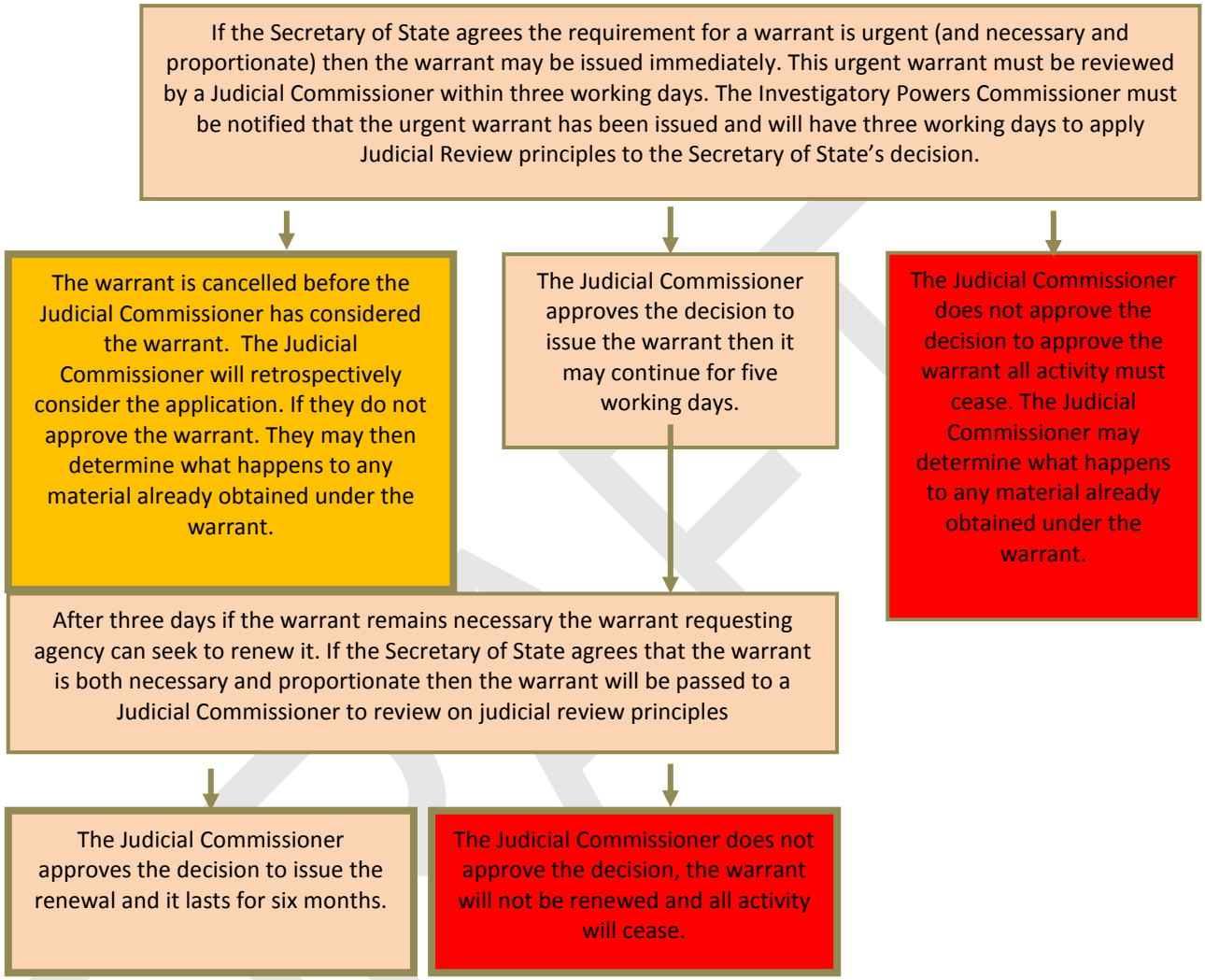
14.2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information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

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

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

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

Annex A – Urgent warrant process



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

It provides guidance on:

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

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

Home Office

Security and Intelligence Agencies' retention and use of bulk personal datasets

Draft Code of Practice

[Autumn] 2016

Security and Intelligence Agencies' retention and use of bulk personal datasets

DRAFT Code of Practice

Pursuant to section 219 and Schedule 7 to the Investigatory Powers Act 2016

[Autumn] 2016

Contents

1 Introduction

1.1 This code of practice relates to the powers and duties conferred or imposed under Part 7 of the Investigatory Powers Act [2016] ("the Act"). It provides guidance on the procedures that must be followed before bulk personal datasets can be retained and examined by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters ("the Security and Intelligence Agencies"). This code of practice is intended for use by the Security and Intelligence Agencies.

1.2 The Act provides that all codes of practice issued under Schedule 6 are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and functions conferred by the Act, it must be taken into account.

1.3 For the avoidance of doubt, the guidance in this code takes precedence over any Security and Intelligence Agency's internal advice or guidance.

2 Scope and definitions

2.1 The Security and Intelligence Agencies need to collect a range of information from a variety of sources to meet the requirements of their statutory functions. They do this in accordance with section 2(2)(a) of the Security Service Act 1989 (SSA) and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 (ISA) ("the information gateway provisions" – see paragraph 11.1 and subsequent paragraphs of Annex A) and through the exercise of various existing statutory powers (see further at paragraph 2.11 and subsequent paragraphs).

2.2 Among the range of information collected are bulk personal datasets ("BPDs"). For the purposes of the Act and this Code, a set of data that has been obtained by a Security and Intelligence agency comprises a BPD where it includes personal data relating to a number of individuals, and the nature of that set is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the Security and Intelligence Agencies in the exercise of their statutory functions. Typically these datasets are very large, and of a size which means they cannot be processed manually.

2.3 Section 183 of the Act specifies that a Security and Intelligence Agency "retains" a BPD for the purposes of the Act if, after any initial examination of the contents, it retains a BPD for the purpose of the exercise of its functions and it holds the BPD electronically for analysis in the exercise of those functions.

2.4 As section 201 makes clear, the initial examination enables the Security and Intelligence Agency, when it comes into possession of a BPD, to carry out a preliminary examination of the contents with a view to establishing whether it is a BPD, and whether that BPD is of a nature that the Security and Intelligence Agency would wish to retain and/or examine it. If so, the Security and Intelligence Agency will consider whether in the light of the dataset's potential intelligence or investigative value, it would be necessary and proportionate to retain the dataset for the purposes of analysis in the exercise of its statutory functions. If it concludes that it would be necessary and proportionate to retain the dataset for these purposes, that retention must be authorised by a BPD warrant. If the dataset is not covered by an existing class BPD warrant, the Security and Intelligence Agency must apply for a specific BPD warrant as soon as reasonably practicable after reaching that conclusion. (See chapters 3 and 4 for further details on these two types of BPD warrant.)

2.5 This initial examination may only be carried out by a Security and Intelligence Agency for these limited purposes, and not for the purposes of any intelligence investigations or operations.

2.6 A Security and Intelligence Agency should complete this initial examination as soon as reasonably practicable. What is 'reasonably practicable' will depend on many different factors. In cases where the Security and Intelligence Agency comes into possession of a BPD which has been created outside of

the UK, there may be a period of time before the Security and Intelligence Agency is in a position to properly assess the data for the purpose of determining whether it wishes to retain or use the BPD (and to apply for a specific warrant, if required). For example, the BPD may need to be brought back to the UK from overseas; the BPD may be in a foreign language; and/or the BPD may be part of a much larger set of data from which it needs to be separated.

2.7 In the light of these considerations, section 201(4) specifies that in cases of BPD created outside of the UK, the acquiring Security and Intelligence Agency has six months from the date on which the head of the intelligence Agency believes a BPD has – or may have been - obtained to conduct the initial examination and, where required, to apply for a specific BPD warrant. Where the BPD is created in the UK, the acquiring Security and Intelligence Agency has three months from the date on which the head of the intelligence services believes that a BPD has – or may have been – obtained to conduct the initial examination and where required apply for a specific BPD warrant.

2.8 Section 201(5) makes it clear that a Security and Intelligence Agency is not in breach of the requirement for a warrant to retain BPD for the period between deciding (as part of the initial examination) that it wants to retain a BPD and the determination of the Security and Intelligence Agency's application for a specific BPD warrant for that BPD. This allows a Security and Intelligence Agency which has received a BPD that falls outside an existing class BPD warrant to retain the dataset while going through the process of obtaining the necessary specific warrant. This is most likely to occur where a BPD is unsolicited (i.e. one which the recipient Security and Intelligence Agency has not requested or sought to obtain), because a Security and Intelligence Agency will not have had the opportunity to assess whether the BPD is covered by a class warrant. However, it could also arise where a solicited BPD is received which contains unexpected material. In such circumstances, the relevant Security and Intelligence Agency should complete its initial examination of the BPD and apply for a specific warrant within the timeframes referred to in section 201(4) (and described in paragraph 2.7 above). Pending issue of the specific warrant, the Security and Intelligence Agency may not examine the BPD for the purposes of any intelligence investigations or operations.

2.9 For the purposes of the Act, 'personal data' has the meaning given to it in section 1(1) of the Data Protection Act 1998 ("DPA" – see also paragraph 11.7 and subsequent paragraphs of Annex A), which defines 'personal data' as follows:

- 'data which relate to a living individual who can be identified –
- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of the data controller (i.e. in this case, the relevant Security and Intelligence Agency), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.

2.10 While the DPA refers to a 'living individual', bulk personal datasets may contain details about individuals who are dead. In the case of some BPDs there may be no indication whether the individuals referred to in the dataset are deceased or not. For example, the electoral roll will inevitably include individuals who are deceased, given that it is not continuously updated: such a dataset would require a warrant under the Act if it had been retained electronically for analysis by a Security and Intelligence Agency in the exercise of its statutory functions. If a BPD contains information about individuals who are known to be deceased, the relevant Security and Intelligence Agency may only decide to retain the dataset if it considers that it would be necessary and proportionate to do so for the purposes of its statutory functions.

Different statutory routes by which BPDs may be acquired

2.11 This code of practice applies not only to BPDs obtained under the information gateway provisions themselves (section 2(2)(a) of SSA and sections 2(2)(a) and 4(2)(a) of ISA), but also to BPDs where the mechanism for obtaining the datasets is subject to authorisation through the exercise of other statutory powers.

2.12 These other statutory powers include, but are not limited to, those exercisable under warrants issued under section 5 of ISA in respect of property interference otherwise than for the purpose of facilitating the obtaining of communications, equipment data or other information; intrusive surveillance warrants issued under section 32 of the Regulation of Investigatory Powers Act 2000 ('RIPA'); directed surveillance authorisations issued under section 28 of RIPA; and covert human intelligence source authorisations issued under section 29 of RIPA. The application of this code of practice to BPDs obtained by exercise of the statutory powers listed above is without prejudice to any additional requirements specified in the legislation relevant to those statutory powers.

2.13 For the avoidance of doubt, this code of practice does not apply to BPDs obtained by a Security and Intelligence Agency when it is exercising a power under a warrant or other authorisation issued or given under the Investigatory Powers Act [2016], for example, under a targeted or bulk interception or equipment interference warrant or under a bulk acquisition warrant (for bulk communications data). BPDs acquired under such other Investigatory Powers Act powers will be subject to the applicable regime under the relevant part of the Act (see also paragraph 3.3 below). This is unless the Security and Intelligence Agency successfully applies to the Secretary of State to give a direction, with Judicial Commissioner approval, to disapply that regime in order to apply the Part 7 regime – see section 203 and paragraph 3.4 below. Once under the Part 7 regime, the provisions of this code of practice will apply.

3 BPDs – general rules

Requirement for authorisation by warrant

3.1 The Act does not create any new power to obtain BPDs. Rather it requires that the retention and use of BPDs must be subject to an authorisation scheme and a comprehensive set of robust and transparent safeguards. Specifically, section 184 of the Act provides that a Security and Intelligence Agency may not exercise a power for the purpose of retaining or examining a BPD unless this is authorised by the issue of a warrant under Part 7 of the Act.

Types of warrant that may be issued

3.2 Section 184(3) describes the two types of warrant provided for by Part 7: a '**class BPD warrant**' authorising a Security and Intelligence Agency to retain, or to retain and examine, BPDs that fall within a class described in the warrant; and a '**specific BPD warrant**' authorising a Security and Intelligence Agency to retain, or to retain and examine, the particular BPD described in the warrant.

Exception to general requirement for authorisation by warrant

3.3 Section 185 explains the specific circumstances in which the general requirement under section 184 for a BPD warrant does not apply. Section 185(1) provides that the Part 7 authorisation scheme does not apply to BPD when this is obtained by a Security and Intelligence Agency by the exercise of **other** powers under the Act, for example, under a targeted or bulk interception or equipment interference warrant. An example of this might be where an email had been intercepted and a BPD was attached to the email. In such cases, the retention and examination of the BPD will be governed by the applicable regime under the relevant part of the Act – for example, the interception regime where a BPD is acquired as a result of interception.

3.4 However, under section 203, a Security and Intelligence Agency can apply to the Secretary of State for a direction that a BPD retained by it under a targeted or bulk interception or equipment interference warrant should have the provisions relating to that other power disapplied, and the provisions of Part 7 of the Act applied instead. Such a direction can only be given with the approval of a Judicial Commissioner. Such a direction can also be varied by the Secretary of State, but again only with the approval of the Judicial Commissioner. Where an application for a direction under section 203 is made by the head of a Security and Intelligence Agency, consideration should also be given to whether an application for a specific warrant should be made

at the same time. An application for a specific warrant should be made if the nature of the BPD which is subject to the direction is BPD that would require a specific warrant under Part 7. Under section 203(12), the Secretary of State may issue a specific warrant at the same time as giving a direction under this section.

3.5 In issuing any direction, the Secretary of State is permitted to provide that any of the associated regulatory provisions which applied to the regime under which the BPD was obtained, should continue to apply once the direction has been issued (with or without modifications). Therefore, in making an application for a direction, a Security and Intelligence Agency should consider which, if any, of the associated regulatory provisions it considers should – or should not – apply to the BPD, if the direction is issued.

3.6 In the case of a BPD obtained by interception which identifies itself as the product of interception, such a direction may not disapply the provisions in section 53 of and Schedule 3 to the Act, which prevent such material from being disclosed in legal proceedings or Inquiries Act proceedings (see section 203(6)(a). Nor may such a direction disapply sections 54-56 of the Act, which impose further restrictions on the disclosure of such material and make it an offence to make an unauthorised disclosure of the existence of an intercept warrant or any intercepted material (see section 203(6)(b)).

3.7 Section 185(2) makes it clear that a BPD can be retained or examined to enable the information contained in it to be destroyed. This provision allows the Security and Intelligence Agencies to hold, temporarily, a BPD which is no longer authorised by a warrant for the purpose only of ensuring that the relevant data is removed from their systems. If a warrant is cancelled or an application for a specific warrant is not approved, it will not always be possible for the Security and Intelligence Agency to delete the BPD immediately from its analytical systems. This is for two reasons. First, as the data has been ingested into wider analytical systems, it may take some time to delete the data – e.g. because the system must be taken off-line and/or because of the need for checks to ensure the correct data is deleted. Secondly, it may be that in some cases only part of a BPD is required to be deleted. This will, as a result, require examination of the dataset first to enable deletion.

3.8 Section 185(3) makes clear that other sections of Part 7 of the Act also provide for exceptions from the requirement to obtain a warrant in particular circumstances. These relate to cases where the Judicial Commissioner has failed to approve an urgent specific BPD warrant but has imposed conditions as to the use or retention of the BPD (section 192(3)(b) – see paragraph 5.34 below); to a time-limited period in which an Agency is conducting an initial examination of a potential BPD (section 201(5) – see paragraph 2.3 above and subsequent paragraphs); and to a limited period after the non-renewal or cancellation of a warrant (section 200(6) – see paragraph 5.59 and subsequent paragraphs).

4 BPD warrant applications

4.1 An application for a BPD warrant is made to the Secretary of State. The requirements set out in Part 7 of the Act only relate to the Security and Intelligence Agencies. An application for a BPD warrant therefore may only be made by or on behalf of the following persons:

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

4.2 All BPD warrants are issued by the Secretary of State. No BPD warrant may be issued unless and until it has been approved by a Judicial Commissioner (see paragraph 5.26 and subsequent paragraphs).

4.3 The only exception to this is a case where the Secretary of State considers that there is an urgent need to issue a specific warrant (see paragraph 5.30 and subsequent paragraphs). Even where the urgency procedure is followed, the Secretary of State still must personally authorise the warrant. In any case where the Secretary of State decides to issue a specific warrant (whether under the urgent procedure or otherwise), he or she must personally sign the warrant where reasonably practicable. However, a designated senior official can sign the warrant if it is not reasonably practicable for the Secretary of State to sign it. When a BPD warrant is issued, it is addressed to the person who submitted the application (or on whose behalf it was submitted).

4.4 Prior to submission, each application should be subject to a review within the Security and Intelligence Agency making the application. This involves consideration as to whether the application is for a purpose falling within sections 187(3)(a)(i) or 188(6)(a)(i) (in the interests of national security), 187(3)(a)(ii) or 188(6)(a)(ii) (for the purpose of preventing or detecting serious crime) or 187(3)(a)(iii) or 188(6)(a)(iii) (in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security). The consideration of the application should also include whether the retention, or the retention and examination, of the BPD is both necessary and proportionate and whether the examination of the BPD is necessary for the operational purposes specified in the application (on which see paragraph 5.7 and subsequent paragraphs). There may be circumstances in which a Security and Intelligence Agency may consider it appropriate to apply for a warrant to retain a BPD before it has physically acquired that BPD.

Applications for class BPD warrants

4.5 Section 187 of the Act explains how the class BPD warrant authorisation process works. It specifies that an application for a class warrant must include:

- a description of the class of BPD to which the application relates; and

- if the Security and Intelligence Agency wishes to examine BPDs of that class, an explanation of the "operational purposes" for which the relevant Security and Intelligence Agency wishes to examine BPDs falling within that class.

Class BPD warrants

4.6 Class BPD warrants are for those datasets which are similar in their content and proposed use and raise similar considerations as to, for instance, the degree of intrusion and sensitivity, and the proportionality of using the data. This allows the Secretary of State to consider the necessity and proportionality of acquiring all data within the relevant class: a class warrant might, for example, authorise a Security and Intelligence Agency to acquire travel datasets that relate to similar routes and which contain information of a consistent type and level of intrusiveness.

4.7 Before submitting an application for a class warrant to the Secretary of State, the Security and Intelligence Agency must be satisfied that:

- retention of BPDs within the class specified in the warrant is **necessary** for one or more of the purposes specified in section 187 of the Act, namely that it is in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- examination of BPDs within that class is **necessary** for one or more of the operational purposes to be specified in the class warrant and for one or more of the statutory purposes specified in section 187 of the Act; and
- examining and retaining BPDs within that class in question is **proportionate** to the functions and purposes referred to in (a) and (b) above; only as much information will be obtained as is necessary to achieve those functions and purposes; and there is no reasonable alternative that will still meet the proposed objective in a less intrusive way.

4.8 Section 187(4) makes clear that the fact that the information that would be obtained under the a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State.

Restriction on use of class BPD warrants

4.9 Section 186 provides that a Security and Intelligence Agency may not retain, or retain and examine, a BPD in reliance on a class BPD warrant if the Head of the Agency considers (a) that the BPD consists of, or includes, **health records**, or (b) that a substantial proportion of the BPD consists of **sensitive personal data**, or (c) that the nature of the BPD, or the circumstances in which it was created, is or are such that its retention, or retention and examination, raises **novel or contentious issues** which ought to be

considered by the Secretary of State and a Judicial Commissioner on an application by the Head of the Agency for a specific BPD warrant.

4.10 'Health record' is defined by section 189(6) to mean a record, or a copy of a record, which (a) consists of information relating to the physical or mental health of an individual, (b) was made by or on behalf of a health professional in connection with the care of that individual, and (c) was obtained by the Security and Intelligence Agency from a health professional or a health service body [or from a person acting on behalf of a health professional or health service body in relation to the record or the copy]. 'Sensitive personal data' is as defined in section 2 of the Data Protection Act 1998: see paragraph 11.8 of Annex A below.

Applications for specific BPD warrants

4.11 Section 188 provides for two sets of circumstances in which a Security and Intelligence Agency may apply to the Secretary of State for a specific BPD warrant. A specific warrant is a warrant for one specific BPD rather than a warrant for a class of BPDs. If either of these two circumstances apply, the relevant Security and Intelligence Agency should consider whether to make an application for a specific warrant.

4.12 In the '*Case 1*' scenario, the dataset does not fall within the scope of an existing class BPD warrant.

4.13 In the '*Case 2*' scenario, the dataset falls within a class of BPD authorised by an existing class warrant, but either (i) the Security and Intelligence Agency is prevented by section 186 from retaining, or retaining and examining, the dataset in reliance on the class BPD warrant (see paragraphs 4.9 and 4.10 above) or (ii) the relevant Security and Intelligence Agency nevertheless considers that it would be appropriate to seek a specific BPD warrant. Examples of the sort of situation where an Security and Intelligence Agency should seek a specific warrant are as follows (with the first two bullets reflecting the provisions of section 186):

- where the dataset consists of, or includes, **health records;** or includes a substantial proportion of **sensitive personal data;** .or
- the nature of the dataset, or the circumstances in which it was created, raise **novel or contentious** issues. An example of this could be where the nature of the BPD is such that its retention, or retention and examination, could raise international relations concerns, which the Agency believes it would be appropriate for the Secretary of State and Judicial Commissioner to consider on an application for a specific warrant.
- The BPD has been assessed by the Security and Intelligence Agency as being relatively more intrusive, such assessment having been carried out in accordance with paragraph 4.17 and subsequent paragraphs.

- The dataset contains confidential information relating to members of sensitive professions. A 'sensitive profession' for these purposes includes lawyers, doctors, journalists, Members of Parliament and Ministers of religion. (References to a Member of Parliament include references to a Member of the UK Parliament, the Scottish Parliament, the Welsh Assembly, the Northern Ireland Assembly and a UK Member of the European Parliament.) (See paragraph 4.19 and subsequent paragraphs.)

4.14 Where section 186 applies, the Security and Intelligence Agency is required by section 188 to include in its application for a specific BPD warrant an explanation of why it is prevented from retaining, or retaining and examining, the BPD in reliance on a class warrant, i.e. it must explain whether this is because the dataset consists of, or includes, health records, or because it includes a substantial proportion of sensitive personal data, or because it raises novel or contentious issues. This should not simply refer back to the statute: it should provide a more detailed explanation of the nature and extent of the material in question, to aid the Secretary of State's understanding of the dataset and the warrant application.

4.15 In the case of a dataset which includes a substantial proportion of sensitive personal data, in its application for the specific BPD warrant the Agency should describe the nature and extent of sensitive personal data in the dataset, where possible by reference to the different categories of sensitive data set out in section 2(a)-(f) of the Data Protection Act 1998 (see paragraph 11.8 in Annex A).

4.16 If required in an individual case, the Security and Intelligence Agency can seek guidance from the Secretary of State (or his or her relevant senior officials) and / or a Judicial Commissioner on whether it would be appropriate for a specific BPD warrant to be sought. The Security and Intelligence Agency should also take into account any guidance provided by the Secretary of State or the Judicial Commissioner in this regard.

Intrusiveness of data

4.17 When considering whether to retain and examine a BPD, the Security and Intelligence Agencies will assess the degree or extent of the intrusiveness which retaining and examining the BPD would involve, that is to say the degree or extent of interference with individuals' right to privacy under Article 8 of the European Convention on Human Rights (ECHR). Each dataset is assessed on a case-by-case basis, and in the round, having regard (amongst other things) to the following factors or indicators:

- Is there an expectation of privacy? Did the individual provide their personal data in confidence to another organisation, not expecting that anyone except that organisation would have access to their data?
- Does the data consist of more than basic personal details (e.g. more than name, date of birth, address, telephone number and e-mail address)?
- Is there information on a person's activities or movements or travel?

- Does the data include 'sensitive personal data' within the meaning of section 2 of the Data Protection Act 1998 ("DPA" - see paragraph 11.8 of Annex A)?
- To what degree does the data, by virtue of its quality, nature or size, mean that, when it is examined, there will be a significant degree of intrusion into the privacy of individuals not of intelligence interest?

4.18 The indicators provide a framework which assists the relevant Security and Intelligence Agency in reaching a decision on the degree or extent of intrusiveness which retaining and examining the dataset would involve. The indicators are not intended to be prescriptive; the presence of one or more will not necessarily result in the dataset as a whole being considered to be relatively more intrusive. (It should be noted that, in accordance with section 186, any dataset containing a substantial proportion of DPA-sensitive data will in any event be required to be authorised by a specific BPD warrant.)

Confidential information relating to members of sensitive professions

4.19 Most BPDs do not include details which would identify someone as a member of a sensitive profession, and do not contain confidential information relating to the sensitive professions. However, in the unlikely event that the Security and Intelligence Agency believed that a BPD contained confidential information relating to a member, or members, of a sensitive profession, the Agency must seek a specific warrant.

4.20 In this context, confidential information would include the content of communications between the professional, acting in their professional capacity, and another party, and any information which identified journalistic sources. Thus, for example, it would include the content of lawyer/client, doctor/patient and MP/constituent communications. However, information relating to a member of a sensitive profession is not, in and of itself, considered confidential. Confidential information in this context would not include the mere fact of membership of the profession, or basic biographical details of a member of the profession. Thus, the fact that a solicitor's telephone number appeared in a telephone directory, would not be considered confidential information.

4.21 Section 188 specifies that an application for a specific BPD warrant must include:

- a description of the specific dataset to which the application relates; and
- an explanation of the "operational purposes" for which the relevant Security and Intelligence Agency wishes to examine the BPD.

4.22 Section 188(6) also enables a Security and Intelligence Agency, when applying for a specific BPD warrant in respect of a particular BPD ('dataset A'), to request at the same time that the authorisation should extend to the retention and use of '**replacement datasets**', i.e. other bulk personal datasets that do not exist at the time of the issue of the warrant but may reasonably be regarded as replacements for dataset A.

4.23 Before submitting an application for a specific warrant to the Secretary of State, the Security and Intelligence Agency must be satisfied that:

- retention of the BPD is **necessary** for one or more of the statutory purposes specified in section 188 of the Act, namely that it is in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- examination of the BPD is **necessary** for one or more of the operational purposes to be specified in the specific warrant and for one or more of the statutory purposes specified in section 188 of the Act; and
- examining and retaining the BPD in question is **proportionate** to what is sought to be achieved by the conduct.

4.24 Section 188(7) makes clear that the fact that the information that would be obtained under the a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State.

5 Authorisation of class and specific BPD warrants by a Secretary of State

5.1 The Secretary of State may only issue a warrant under sections 187 (class BPD warrants) or 188 (specific BPD warrants) if the Secretary of State considers the following tests are met:

- The warrant is necessary:[1]
  - In the interests of national security;
  - For the purpose of preventing or detecting serious crime; or
  - In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security.
- The conduct authorised by the warrant is proportionate to what it seeks to achieve.
- Each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary; and the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in section 187(3)(a) or section 188(6)(a). (See paragraph 5.7 and subsequent paragraphs for more on operational purposes.)
- There are satisfactory safeguards in place. The Secretary of State must consider that satisfactory arrangements are made for storing the BPD and for protecting them from unauthorised disclosure. (See paragraph 7.3 and subsequent paragraphs).

5.2 A Judicial Commissioner has approved the issue of the warrant. Except in the case of an urgent specific warrant, the Secretary of State may not issue a warrant unless and until the decision to issue the warrant has been approved by a Judicial Commissioner (see paragraph 5.26 and subsequent paragraphs).

5.3 When considering whether to issue a class BPD warrant, the Secretary of State will have regard to:

- the nature and scope of the class for which the warrant is being sought, i.e. the category of data and breadth or width of the class, the necessity and proportionality considerations, and any other factors specified in paragraph 4.6 which apply; and
- the number of individual bulk personal datasets which are likely to fall within that class warrant.

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

5.4 The Secretary of State will not issue the warrant unconditionally unless satisfied that:

- having regard to the considerations referred to in the first bullet point in paragraph 5.3 above, it is appropriate to issue the warrant; and
- the number of bulk personal datasets referred to in the second bullet point in paragraph 5.3 above is such that it will still be possible for the Secretary of State and Judicial Commissioner, including the Investigatory Powers Commissioner, to exercise effective oversight of the operation of the class BPD warrant and of the retention and use of the individual BPDs authorised by that warrant.

5.5 In the event that the Secretary of State is satisfied in relation to the two bullet points in paragraph 5.4 above, he or she will issue the warrant.

5.6 In the event that the Secretary of State is not satisfied in relation to either bullet-point, he or she will either require the boundaries of the class to be reduced and/or (as the case may be) specify what the upper limit of BPDs in the class ('the cap') should be. He or she would do this by either (a) refusing to issue the warrant and instead inviting the relevant Security and Intelligence Agency to split the class into smaller classes and submit revised applications for class BPD warrants accordingly, or (b) issuing the class BPD warrant subject to the specified cap and inviting the relevant Agency to submit applications for a separate class BPD warrant or specific BPD warrants for any individual BPDs which could not be included in the class warrant that has been issued without exceeding the cap specified for that class.

What are operational purposes?

5.7 Section 202 provides specific safeguards relating to the selection of data contained in a BPD under class or specific BPD warrant for examination. References to examination of data from a BPD are references to it being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant (see section 239 of the Act for general definitions in the Act).

5.8 Sections 202(1) and 202(2) make clear that selection for examination of data from a BPD may only take place for one or more of the operational purposes that are specified on the warrant. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination, rather than limiting the information which can be examined per se, and no official is permitted to select for examination, data from a BPD, otherwise than in accordance with a specified operational purpose. For the avoidance of doubt, data from a BPD selected for an operational purpose can, where it is necessary and proportionate to do so, be used, disclosed and retained for any statutory purpose.

5.9 Sections 187 and 188 make clear that operational purposes must relate to one or more of the statutory purposes specified on the warrant. However, section 194(5) provides that the operational purposes specified in the warrant must be ones specified in the list of operational purposes which the Heads of

the Security and Intelligence Agencies are required to maintain. Section 194(6) makes clear that a warrant may specify all the operational purposes that appear on that list of operational purposes. Section 194(7) and 194(8) provide that an operational purpose may be specified in that list only with the Secretary of State's approval, which may only be given if the Secretary of State is satisfied that the operational purpose is specified in a greater level of detail than the wording of one of the statutory purposes. Thus, operational purposes provide the Secretary of State and the Judicial Commissioner with a more granular understanding of the purposes for which the BPD will be retained and examined by the Security and Intelligence Agencies.

5.10 Section 194(9) provides that every three months (from when that provision comes into force) the Secretary of State must give a copy of the list of operational purposes to the Intelligence and Security Committee of Parliament. Section 194(11) requires the Prime Minister to review the list of operational purposes at least once a year.

5.11 The Security and Intelligence Agencies need to retain the operational agility to respond to developing and changing threats and the range of operational purposes that may need to be specified on a BPD warrant needs to reflect this. New operational purposes will therefore be required over time. The Act provides (under section 197) that a BPD warrant may be modified to amend the operational purposes specified on it; for further detail on the process for this, see later sections of this chapter.

5.12 In line with this, the Security and Intelligence Agencies will need to ensure the full range of their BPD warrants are relevant to the current threat picture and, where applicable, the intelligence priorities set by the National Security Council. They will need to identify operational purposes that need to be added to or removed from BPD warrants, including in urgent circumstances. This would be done through the modifications process set out in the Act.

5.13 Some operational purposes that may need to be specified on a bulk warrant will be consistent across the three Agencies, although some purposes will be relevant to a particular Agency or two of the three. Operational purposes should as far as possible be consistent across the bulk capabilities provided for by the Act.

5.14 The Act does not limit the number of operational purposes that may be specified in the warrant. Where the necessity and proportionality test is satisfied, a warrant may include all operational purposes currently in use by an Agency. BPDs are likely to have potential relevance and utility across the full range, or most, of a Security and Intelligence Agency's operations or investigations. In the majority of cases, it will therefore be highly likely that it would be considered necessary for BPD warrants to specify the full range of an Agency's operational purposes.

5.15 An example of an "operational purpose" in the context of the security and intelligence agencies' international counter-terrorism work might be 'The Investigation, assessment and disruption of attack planning by Daesh in Iraq/Syria against the UK.'

Necessity and proportionality

5.16 Where the retention or examination of a BPD involves an interference with an individual's rights under Article 8 (right to respect for private and family life) of the ECHR, this will only be justifiable if the interference is necessary and proportionate. The Act recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the statutory purposes set out in section 187(3) and 188(6) of the Act:

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

5.17 The Secretary of State must also believe that the retaining or examination of the BPD is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into privacy against the need for the activity in investigative, operational or capability terms.

When will retaining or examining a BPD be necessary?

5.18 What is necessary in a particular case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the 'necessity' requirement in relation to retention and examination, the Security and Intelligence Agencies and the Secretary of State must consider why retaining or retaining and examining the bulk personal dataset is 'really needed' for the statutory and operational purposes referred to in paragraph 5.1 above.

5.19 Chapter 7 includes further material on the necessity considerations that apply to examination of BPDs.

When will retaining or examining a BPD be proportionate?

5.20 The retention or examination of the bulk personal dataset must also be proportionate to what is sought to be achieved by the conduct authorised under the warrant. In order to meet the 'proportionality' requirement, the Security and Intelligence Agencies and the Secretary of State must balance (a) the level of interference with the individual's right to privacy, both in relation to subjects of interest who are included in the relevant data and in relation to other individuals who are included in the dataset and who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the dataset.

5.21 The Security and Intelligence Agency and the Secretary of State must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the dataset and the importance of the operational purposes to be achieved. The

Security and Intelligence Agency and the Secretary of State must also consider whether there is a reasonable alternative that will still meet the proposed objective – i.e. which involves less intrusion.

5.22 The warrant will not be proportionate if it is excessive in the overall circumstances of the case. The conduct authorised should bring an expected benefit to the Security and Intelligence Agency's investigations or operations and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not necessarily render intrusive conduct proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

5.23 Chapter 7 includes further material on the proportionality considerations that apply to examination of BPDs.

Authorisation of a specific warrant: senior officials

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

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

Approval of the issue of BPD warrants by a Judicial Commissioner

5.26 Before a class or specific BPD warrant can be issued by the Secretary of State, it must be approved by a Judicial Commissioner.

5.27 Section 190 of the Act provides that, when deciding whether to approve the decision to issue a BPD warrant, the Judicial Commissioner must review the Secretary of State's conclusions as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. The Judicial Commissioner must also review the Secretary of State's conclusions as to whether each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary, and whether the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in section 187(3)(a) or section 188(6)(a). In reviewing these matters, the Judicial Commissioner must apply judicial review principles. The Judicial Commissioner must also consider the matters sufficiently carefully so as to ensure he or she complies with the duties set out in section 2 (general duties in relation to privacy). The Judicial Commissioner may speak to the warrant granting department or warrant seeking agency as part of their considerations.

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

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

5.29 If the Investigatory Powers Commissioner refuses the decision to issue a warrant the Secretary of State must not issue the warrant. There is no avenue of appeal available to the Secretary of State.

Urgent authorisations

5.30 The Act makes provision (see sections 191 – 193) for cases in which a specific BPD warrant is required urgently. It is not possible to seek an urgent class BPD warrant.

5.31 In addition to the tests sets out at paragraph 5.1 above, the Secretary of State must believe that there was an urgent need to issue the warrant. Urgency is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the requisite time. Accordingly, urgent warrants can be issued by the Secretary of State without prior approval from a Judicial Commissioner. The requisite time would reflect when the authorisation needs to be in place to meet an operational or investigative need. Urgent warrants should, therefore, fall into at least one of the following three categories:

- Imminent threat to life or serious harm – for example, an individual has been kidnapped and it is assessed that his life is in imminent danger;

- A significant intelligence gathering opportunity which is significant because of the nature of the potential intelligence, the operational need for the intelligence is significant, or the opportunity to gain the intelligence is rare or fleeting – for example, a group of terrorists is about to meet to make final preparations to travel overseas.
- A significant investigative opportunity – for example, there is an imminent attempt to smuggle weapons into the UK to a known terrorist by boat; we may wish to use BPD to identify the vessel to prevent the weapons reaching the terrorist.

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

5.33 If the Judicial Commissioner retrospectively agrees to the Secretary of State's issuance of the urgent warrant, and it is still considered necessary and proportionate by the warrant requesting agency, renewal of the urgent warrant may be sought. A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed. If it is renewed it expires after six months, in the same way as non-urgent BPD warrants.

5.34 The Judicial Commissioner may refuse to approve the Secretary of State's decision to issue the urgent warrant. If that is the case, the urgent warrant ceases to have effect and may not be renewed. However, the Judicial Commissioner may:

- direct that any BPD retained in reliance on the warrant must be destroyed; or
- impose conditions as to the use or retention of any such datasets. The Security and Intelligence Agency or the Secretary of State can make, or be required to make by the Judicial Commissioner, representations to the Commissioner about requirements to destroy datasets and/or conditions relating to use or retention.

5.35 A Security and Intelligence Agency is not to be regarded as in breach of the requirement to have a warrant where it retains or (as the case may be) examines a bulk personal dataset in accordance with conditions imposed by the Judicial Commissioner in the way described in paragraph 5.34 above.

5.36 If the Judicial Commissioner does not approve the urgent warrant, the relevant Security and Intelligence Agency must do whatever is reasonably practicable to ensure that anything in the process of being done under the warrant stopped as soon as possible. In such a scenario, activity undertaken by virtue of that urgent warrant remains lawful, including activity in process at the time the warrant ceases to have effect which it is not reasonably practicable to stop.

5.37 A flowchart setting out the urgent authorisation process is provided at Annex B.

Duration of BPD warrants

5.38 Section 195 provides that, for non-urgent warrants, the warrant comes into effect at the point at which it is issued or, in the case of a renewed warrant, the day following the day on which it would otherwise have ceased to have effect. In either case, the warrant lasts for six months. Such warrants may only be renewed in the last 30 days of the period for which they have effect. An urgent warrant lasts for five working days after the day on which it was issued.

5.39 Where modifications to a BPD warrant are made, the warrant expiry date remains unchanged.

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

Modification of a BPD warrant

5.41 Section 197 provides for modifications of BPD warrants. There are two kinds of modifications: (a) major modifications, which add or vary any operational purpose specified in the warrant; and (b) minor modifications, which remove any operational purpose specified in the warrant. A class or specific BPD warrant may be modified by an instrument under the provisions at section 197.

5.42 A modification to add or vary an operational purpose must be made by the Secretary of State (except in the situation described in paragraph 5.43 below), and except where the Secretary of State considers it urgent, the decision to make the modification must be approved by a Judicial Commissioner before the modification comes into force. (See paragraph 5.46 and subsequent paragraphs for more on urgent modifications.) A modification to remove an operational purpose may be made by Secretary of State or a designated senior official acting on behalf of the Secretary of State.

5.43 If it is not reasonably practicable for the Secretary of State to make a modification to add or vary an operational purpose – for example where he or she is out of the country, working within his or her constituency, or otherwise unavailable – a senior official acting on behalf of the Secretary of State may make the modification with the express authorisation of the Secretary of State. In such a case, the modification instrument must contain a statement (a) that it is not reasonably practicable for the instrument to be signed by the Secretary of State and (b) that the Secretary of State has personally and expressly authorised the making of the modification.

5.44 If a modification removing an operational purpose is made by a designated senior official, the Secretary of State must be notified personally of the modification and the reasons for making it. This can be done in writing or orally, though if it is done orally a record must be kept (see Chapter 8 of this Code for further information on record-keeping). It should happen as quickly as reasonably practicable. If at any time the Secretary of State, or a senior

official acting on their behalf, considers that a specified operational purpose is no longer necessary in the interests of the statutory purposes listed on the warrant, they must modify the warrant to remove that operational purpose.

5.45 The modification instrument should be addressed to the person to whom the warrant was issued (i.e. the head of the relevant Security and Intelligence Agency).

Urgent modification of a BPD warrant

5.46 Sections 197 and 198 provide for urgent modifications of BPD warrants. An operational purpose may be added to or varied on an urgent basis. In such a case, the Secretary of State's decision to make the modification does not need to be approved by a Judicial Commissioner prior to having effect. A Judicial Commissioner must decide whether to approve the decision to make such a modification within five working days.

5.47 If the Judicial Commissioner does not approve the urgent modification, the warrant has effect as if the modification had not been made, and the relevant Security and Intelligence Agency must do whatever is reasonably practicable to ensure that anything in the process of being done under the warrant by virtue of that modification is stopped as soon as possible. In such a scenario, activity undertaken by virtue of that modification remains lawful, including activity in process at the time the modification ceases to have effect which it is not reasonably practicable to stop.

Renewal of BPD warrants

5.48 The Secretary of State may renew a warrant. Non-urgent warrants may only be renewed in the last 30 days of the period for which they have effect. Urgent warrants may be renewed at any point before their expiry date (section 196 of the Act). Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 5.1 above. In particular, the applicant must give an assessment of the value derived to date from the specific BPD or from the class of BPD in question, and explain why it continues to be necessary to retain and/or examine the specific BPD(s) or the class of BPDs, and why this continues to be proportionate.

5.49 In deciding whether to renew a BPD warrant, the Secretary of State must also consider whether the examination of the specific BPD or the class of BPDs continues to be necessary for one or more of the specified operational purposes, and that any examination of that material for these purposes is necessary for one or more of the statutory purposes (as set out in the first bullet-point in paragraph 5.1 above) on the warrant.

5.50 When considering whether to renew a class BPD warrant, the Secretary of State will have regard to:

- the nature and scope of the class for which the warrant is being sought, i.e. the category of data and breadth or width of the class, the necessity and proportionality considerations, and any other factors specified in paragraph 4.6 which apply; and
- the number of individual bulk personal datasets which are likely to fall within that class warrant.

5.51 The Secretary of State will not issue the warrant unconditionally unless satisfied that:

- having regard to the considerations referred to in the first bullet point in paragraph 5.50 above, it is appropriate to issue the warrant; and
- the number of bulk personal datasets referred to in the second bullet point in paragraph 5.50 above is such that it will still be possible for the Secretary of State and Judicial Commissioner, including the Investigatory Powers Commissioner, to continue to exercise effective oversight of the operation of the class BPD warrant and of the retention and use of the individual BPDs authorised by that warrant.

5.52 In the event that the Secretary of State is satisfied in relation to the two bullet points in paragraph 5.51 above, he or she will issue the warrant.

5.53 In the event that the Secretary of State is not satisfied in relation to either bullet-point, he or she will either require the boundaries of the class to be reduced and/or (as the case may be) specify what the upper limit of BPDs in the class ('the cap') should be. He or she would do this by either (a) refusing to issue the warrant and instead inviting the relevant Security and Intelligence Agency to split the class into smaller classes and submit revised applications for class BPD warrants accordingly, or (b) issuing the class BPD warrant subject to the specified cap and inviting the relevant Agency to submit applications for a separate class BPD warrant or specific BPD warrants for any individual BPDs which could not be included in the class warrant that has been issued without exceeding the cap specified for that class.

5.54 Where the Secretary of State is satisfied that the retention and/or examination of the BPD continues to meet the requirements of the Act, the Secretary of State may renew the warrant. In all cases, a BPD warrant may only be renewed if the decision to renew that warrant has been approved by a Judicial Commissioner. The renewed warrant is valid for six months from the day following the day on which it would otherwise have ceased to have effect.

5.55 A renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Cancellation of warrant

5.56 The Secretary of State, or a senior official acting on his or her behalf, may cancel a BPD warrant at any time (see section 199). Such persons must cancel a BPD warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on the grounds of any one of the statutory purposes for which it was issued. The Security and Intelligence

Agencies will therefore need to keep their BPD warrants under continuous review and must notify the Secretary of State if they assess that a warrant is no longer necessary. In practice, the responsibility to cancel a warrant will normally be exercised by a senior official in the warrant granting department on behalf of the Secretary of State.

5.57 The cancellation instrument will be addressed to the person to whom the warrant was issued.

5.58 The cancellation of a warrant does not prevent the Secretary of State deciding, with Judicial Commissioner approval, to issue a new warrant, covering the same or different bulk personal datasets and operational purposes, in the future should it be considered necessary and proportionate to do so. Where there is a requirement to modify the warrant, other than to amend the operational purposes for which the data can be examined, then the warrant may be cancelled and a new warrant issued in its place.

Non-renewal or cancellation of class BPD warrants

5.59 Section 200 provides for the situation where a BPD warrant is not renewed or is cancelled and, in particular, sets out the process for dealing with the material that was retained under the warrant in question. The material may be destroyed; section 200(2) ensures retention or examination of the material for the purpose of deleting the material is lawful. But depending on the reasons why the warrant has been cancelled or not renewed, the relevant Security and Intelligence Agency may consider it necessary and proportionate to retain some or all of the material that had been retained under the authority of that warrant. Section 200 therefore includes bridging provisions to ensure any retention and examination of the material in question is lawful pending any authorisation via a new warrant. The relevant Security and Intelligence Agency may apply for a new class or specific BPD warrant within five working days (section 200(2)).

5.60 If the relevant Agency needs further time to consider whether to apply for a new warrant, it may instead apply to the Secretary of State for authorisation to retain or retain and examine some or all the material retained under the warrant. The Agency can only apply for such authorisation if it is considering whether to apply for a new class or specific BPD warrant to authorise retention or retention and examination of the material. In particular, under section 200(6) and 200(7), the Agency has five working days in which to decide whether it wants to apply for such authorisation. Retention and examination of that data is lawful pending the Secretary of State's decision under such an application. If the agency so applies, the Secretary of State can then direct that any of the material should be destroyed or, with the approval of the Judicial Commissioner, can authorise the retention or examination of any of the material, subject to such conditions as the Secretary of State considers appropriate. Retention or examination is lawful under such a direction. During that period, the agency must consider whether to and then apply for a new warrant as soon as reasonably practicable and in any event within three months. Retention and examination remains lawful for the period between the agency applying for a new warrant and the determination of that

application, even if determination takes place after the end of the three month period.

5.61 These provisions may be required if, for example, the Secretary of State is no longer satisfied that all the individual bulk personal datasets in a BPD class authorised by a warrant should be retained, because e.g. the class is considered too wide in scope, but would be willing to issue to the relevant Security and Intelligence Agency a class BPD warrant for a more restricted class of BPD (or a specific warrant). In such a situation, the Secretary of State might be satisfied that it was necessary and proportionate for the relevant Intelligence Agency to retain some of the individual bulk personal datasets in the BPD class or a subset or subsets of that material, pending the issue of a new class warrant or specific warrant. Or the Secretary of State may be willing to authorise the continued retention and examination of some but not all the material held under a specific BPD warrant.

5.62 If the Judicial Commissioner does not approve a decision to authorise the continued retention or examination of any of the material, section 200(4) requires that he or she must give the Secretary of State written reasons for this. If it was a Judicial Commissioner other than the Investigatory Powers Commissioner who did not approve the decision, the Secretary of State can ask the Investigatory Powers Commissioner to decide whether to approve the decision (section 200(5)).

6 Authorisation of the retention and use of BPDs falling within a class BPD warrant

6.1 For the purpose of dealing with BPD falling within the scope of an existing class BPD warrant, each Security and Intelligence Agency should have a formal internal authorisation procedure which must be complied with.

6.2 Before deciding to retain a BPD falling within the scope of an existing class BPD warrant ("the relevant class warrant") for the purpose of the exercise of its statutory functions, the Security and Intelligence Agency must be satisfied that:

- the BPD in question falls within the scope of the relevant class warrant;
- the Agency must be satisfied that it is not prevented by section 186 from retaining, or retaining and examining, the dataset in reliance on the class BPD warrant (see paragraph 4.9 and subsequent paragraphs);
- retention of the BPD is **necessary** for one or more of the relevant Agency's statutory functions;
- each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary; and the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in section 187(3)(a) or section 188(6)(a)
- retaining and examining the BPD in question is **proportionate** to what is sought to be achieved by the conduct;
- only as much information will be obtained as is **necessary** to achieve those functions and purposes; and
- there is no reasonable alternative that will still meet the proposed objective in a less intrusive way.

6.3 An explanation of the necessity and proportionality tests is provided at paragraph 5.16 and subsequent paragraphs and of operational purposes at paragraph 5.7 and subsequent paragraphs.

6.4 Before a new dataset falling within the scope of a class BPD warrant is held electronically by a Security and Intelligence Agency for analysis in the exercise of its functions, the relevant staff in that Agency should consider the factors set out in paragraph 6.2 above and complete the formal internal authorisation procedure. The authorisation procedure involves an application to a senior manager which should include the following:

- a description of the particular BPD, including details of the personal data contained in the dataset, and any confidential information relating

to members of sensitive professions or data that is considered to be intrusive (as assessed by reference to the factors in paragraph 4.17 and subsequent paragraphs) of which staff are aware;

- a description of the class BPD warrant within which the dataset falls;
- the justification for retention and examination, including the operational purposes for which examination of the dataset is required, the statutory functions which are engaged and the necessity and proportionality of the proposed retention and examination;
- an assessment of the level of intrusion into privacy;
- the consideration and advice of the relevant Agency's legal advisers; and
- the extent of political, reputational or other risk.

6.5 The relevant Security and Intelligence Agency should consult line or senior management for guidance. They may also seek guidance from relevant Senior Officials (i.e. members of the Senior Civil Service in the relevant warrant-issuing Department), the Secretary of State and/or the Investigatory Powers Commissioner. If the Security and Intelligence Agency is not clear on whether an internal authorisation is appropriate, then they should seek guidance from the Secretary of State (or his or her relevant senior officials) and / or a Judicial Commissioner. The Security and Intelligence Agency should also take into account any guidance provided by the Secretary of State or the Judicial Commissioner in this regard.

6.6 Once authorised, the completed application should be stored on a record by the appropriate Security and Intelligence Agency's information governance/compliance team, which will include the date of approval. This record should also contain the date when the Agency decided to retain the dataset after the initial examination referred to in paragraph 2.3 and subsequent paragraphs, which should be the date used for the review process (for which see paragraph 7.18 and subsequent paragraphs).

7 Safeguards

7.1 This chapter sets out the safeguards which each Security and Intelligence Agency should put in place in relation to storage of bulk personal datasets (whether acquired under class BPD or specific BPD warrants), record-keeping, access to and examination of BPDs, disclosure and review and retention of BPDs. The Secretary of State may only issue a BPD warrant if s/he considers that arrangements made by the relevant Security and Intelligence Agency for storing BPD and for protecting the datasets from unauthorised disclosure are satisfactory (as set out in sections 187(3)(d) and 188(6)(d)).

7.2 The safeguards in this chapter are in addition to those set out in earlier chapters of this code, including the requirement for the retention and examination of a BPD to be necessary and proportionate for it to take place; the need to ensure only as much information will be obtained as is necessary and that there is no reasonable alternative that will still meet the proposed objective in a less intrusive way; the particular considerations that need to be given to the intrusiveness of the data and the extent to which that data includes confidential information relating to sensitive professions; and the requirement for Secretary of State and Judicial Commissioner approval for BPD warrants. (See chapters 4 and 5).

Storage

7.3 Each Security and Intelligence Agency should maintain robust data security and protective security standards. They should have in place handling procedures so as to ensure that the integrity and confidentiality of the information in the BPD is effectively protected, that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that it is detected and that appropriate disciplinary action is taken. In particular, each Agency should apply the following protective security measures:

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

Safeguards before a BPD is made accessible

7.4 Where a BPD contains either material assessed by the Security and Intelligence Agency as relatively more intrusive (see paragraph 4.17 and

subsequent paragraphs) or confidential information relating to sensitive professions (see paragraph 4.19 and subsequent paragraphs), before such a BPD is held electronically by a Security and Intelligence Agency for analysis in the exercise of its functions the relevant Agency should consider whether access by its staff to such data should be subject to any particular restrictions, including sensitive fields being suppressed or deleted, or additional justification required to access and examine sensitive data-fields.

Access and examination

7.5 In relation to information held in bulk personal datasets, each Security and Intelligence Agency should have in place the following additional measures:

- Access to and examination of the information contained within the bulk personal datasets should be strictly limited to those with an appropriate business requirement to use these data;
- Individuals may only access information within a bulk personal dataset if examination of the BPD is necessary for one or more of the operational purposes specified in the relevant class warrant or specific warrant and for one or more of the relevant statutory purposes specified in the Act (see paragraph 5.16 and subsequent paragraphs);
- If individuals access information within a bulk personal dataset with a view to subsequent disclosure of that information, (in addition to satisfying the condition in the above bullet) they may only access and examine the relevant information if such disclosure is necessary for the performance of the statutory functions of the relevant Intelligence Agency or for the additional limited purposes set out in the information gateway provisions (sections 2(2)(a) and 4(2)(a) of the ISA and section 2(2)(a) of the SSA – see paragraph 11.3 of Annex A);
- Before accessing or disclosing information, individuals must also consider whether to do so would be proportionate (as described in paragraph 5.20 and subsequent paragraphs and below). For instance, they must consider whether other, less intrusive methods can be used to achieve the desired outcome;
- Users should receive mandatory training regarding their professional and legal responsibilities, including the application of the provisions of the Act and this Code of Practice. Refresher training and/or updated guidance should be provided when systems or policies are updated;
- Each Security and Intelligence Agency should ensure that there is a system in place whereby the relevant audit team effectively monitors the examination of bulk personal data by staff in order to detect misuse or identify activity that may give rise to security concerns;
- Appropriate disciplinary action should be taken in the event of inappropriate behaviour being identified;

- Users should be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution; and
- The Secretary of State must ensure that the safeguards are in force before any BPD warrant authorising use can begin.

7.6 The Security and Intelligence Agencies should also take the following measures – by establishing the necessary underpinning working practices - to reduce the level of interference with privacy arising from the retention and examination of bulk personal datasets:

- Minimising the number of results which are presented for analysis, by training and requiring staff to frame queries in a proportionate way; and
- If necessary, confining access to specific datasets (or subsets thereof) to a limited number of analysts.

Personnel security

7.7 All persons within the Security and Intelligence Agencies who may have access to BPDs or need to see any reporting in relation to them 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 BPDs to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

Additional access safeguards for confidential information relating to sensitive professions

7.8 The Security and Intelligence Agencies should ensure that, before Security and Intelligence Agency staff who are searching a bulk personal dataset specifically target for access or examination confidential information relating to members of sensitive professions, **special consideration** is given to the necessity and proportionality justification for the interference with privacy that will be involved.

7.9 The Security and Intelligence Agencies should also ensure that particular care is taken when deciding whether to seek such access to data or information of the kind described in paragraph 7.8 above, and should consider whether there might be unintended consequences of such access and whether the public interest is best served by this, and only to do so if authorised beforehand by a senior manager.

7.10 All cases where Security and Intelligence Agency staff intentionally seek to examine such data or information, they should be required to record the fact that such information or data has been accessed and selected and flag this to the Investigatory Powers Commissioner at the next inspection. Likewise, where Security and Intelligence Agency staff are aware that in searching a

bulk personal dataset they have unintentionally accessed such data or information but have decided to select and retain it, they should be required to record the fact of this access and intentional selection and flag this to the Investigatory Powers Commissioner at the next inspection.

Disclosure

7.11 Information in bulk personal datasets held by a Security and Intelligence Agency (whether acquired under class BPD or specific BPD warrants) may only be disclosed to persons outside the relevant Agency if the following conditions are met:

- that the objective of the disclosure falls within the Agency's statutory functions or is for the additional limited purposes set out in the information gateway provisions (sections 2(2)(a) and 4(2)(a) of the ISA and section 2(2)(a) of the SSA – see paragraph 11.3 of Annex A);
- that it is **necessary** to disclose the information in question in order to achieve that objective;
- that the disclosure is **proportionate** to the objective; and
- that only as much of the information will be disclosed as is **necessary** to achieve that objective.

7.12 In order to meet the 'necessity' requirement in relation to disclosure, the Security and Intelligence Agency must be satisfied that disclosure of the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of that Agency or for the additional limited purposes set out in the information gateway provisions.

7.13 The disclosure of the bulk personal dataset must also be proportionate to the purpose in question. In order to meet the 'proportionality' requirement, the relevant Security and Intelligence Agency must be satisfied that the level of interference with the individual's right to privacy is justified by the benefit to the discharge of the Agency's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. The relevant Security and Intelligence Agency must consider whether there is a reasonable alternative that will still meet the proposed objective – i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole bulk personal dataset.

7.14 Before disclosing any bulk personal data, the relevant Security and Intelligence Agency must either take reasonable steps to ensure that the intended recipient organisation has, and will maintain, satisfactory arrangements regarding the use of the BPD, and for safeguarding the confidentiality of the data and ensuring that it is securely handled. What steps should to be viewed as reasonable in any particular instance of disclosure will depend on the circumstances of the case, but will include consideration of the nature of the disclosure and what is known about the recipient.

7.15 Where the BPD has been acquired under an interception warrant, the relevant Security and Intelligence Agency must also consider whether the restrictions on the use of disclosure of material obtained under an interception warrant into legal proceedings, will be relevant (see section 203(6)).

7.16 These conditions for disclosure apply equally to the disclosure of an entire bulk personal dataset, a subset of the dataset, or an individual piece of data from the dataset. Disclosure of the whole (or a subset) of a bulk personal dataset is subject to internal authorisation procedures in addition to those that apply to an individual item of data. The authorisation process requires an application to a senior manager designated for the purpose which is required to set out the following:

- a description of the dataset it is proposed to disclose (in whole or in part), including details of the personal data contained in the dataset, and any significant component of intrusive data or confidential information relating to sensitive professions of which staff are aware;
- the operational and legal justification for the proposed disclosure, and the necessity and proportionality of the disclosure;
- an assessment of the level of intrusion into privacy;
- the extent of political, reputational or other risk;
- whether any caveats or restrictions should be applied to the proposed disclosure; and
- confirmation that reasonable steps have been taken to ensure that disclosure to the recipient organisation is in accordance with paragraph 7.14 above.

7.17 This information should be included, so that the senior manager can then consider the factors in paragraph 7.11 with operational, legal and policy advice taken as appropriate. In difficult cases, the relevant Intelligence Agency may seek guidance from relevant Senior Officials (i.e. members of the Senior Civil Service in the relevant Department), the Secretary of State and/or the Investigatory Powers Commissioner.

Review of retention and deletion

7.18 Each Security and Intelligence Agency must regularly review the operational and legal justification for its **continued retention, examination and use** of each bulk personal dataset retained by it under a class warrant. The frequency of the review – as agreed with the Secretary of State – should be guided by the level of intrusion which is generated by the holding of the BPD (and any other factors that the Security and Intelligence Agency or the Secretary of State consider appropriate), and must in any event be such as to ensure that the justification for the continued retention of bulk personal datasets covered by the relevant class warrant is adequately considered.

7.19 The retention and review process requires consideration of the following factors:

- The operational and legal justification for continued retention, including its necessity and proportionality;
- Whether such information could be obtained elsewhere through less intrusive means;
- An assessment of the value of the dataset and its examination for the operational purposes, with examples of use;
- The extent to which the dataset originally acquired needs to be replaced by a more up-to-date;
- The level of intrusion into privacy;
- The extent of political, reputational or other risk; and
- Whether any caveats or restrictions should be applied to continued retention.

Destruction

7.20 Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies of it held within the relevant Security and Intelligence Agency should be destroyed. Section 239 of the Act provides definition of 'destroy'. Each Agency should report to the Secretary of State, on a six-monthly basis, with a list of all BPDs destroyed in the previous six months.

Other management controls

7.21 The retention and disclosure of a bulk personal dataset should be subject to scrutiny in each Security and Intelligence Agency, which should put in place an effective system to ensure each of the following:

- that each bulk personal dataset has been properly obtained;
- that access to a BPD is permitted only for the specified operational purposes and for the relevant Security and Intelligence Agency's statutory functions;
- that any disclosure is properly justified; and
- that retention and examination of the BPD remains necessary for the specified operational purposes and the proper discharge of the relevant Security and Intelligence Agency's statutory functions and is proportionate to achieving that objective.

7.22 Each Security and Intelligence Agency should ensure that there is a system in place whereby the relevant audit team effectively monitors the examination of bulk personal datasets by staff in order to detect misuse or identify activity that may give rise to security concerns.

7.23 Any such identified activity initiates a formal investigation process in which legal, policy and Human Resources input will be requested where appropriate.

Failure to provide a valid justification for a search may result in disciplinary action, which in the most serious cases could lead to dismissal and/or the possibility of prosecution.

7.24 All reports on audit investigations are required to be made available to the Investigatory Powers Commissioner for scrutiny (see chapter 9 below).

8 Record-keeping and error-reporting

8.1 The oversight regime allows the Investigatory Powers Commissioner to inspect the warrant application upon which the authorisation was based, and the applicant may be required to justify the content. Each Security and Intelligence Agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:

- All applications made for BPD warrants and all applications made for the renewal of such warrants;
- All BPD warrant instruments, associated schedules, renewal instruments and copies of modification applications; and
- Where any application is refused, the grounds for refusal as given by the Secretary of State.

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

- All advice provided to the Secretary of State to support his/her consideration as to whether to issue or renew the BPD warrant;
- Written records, including contemporaneous notes, of requests for urgent authorisations of warrants or modifications; and
- Where the issuing of any application is not approved by the Judicial Commissioner, the grounds for refusal as given by the Judicial Commissioner and any associated advice / applications to the Investigatory Powers Commissioner if there is an appeal.

8.3 Each Security and Intelligence Agency must also keep a record of the following information to assist the Investigatory Powers Commissioner to carry out his/her statutory functions:

- The number of applications for (a) class and (b) specific BPD warrants submitted.
- The number of applications for (a) class and (b) specific BPD warrants refused by the Secretary of State.
- The number of decisions to issue (a) class and (b) specific BPD warrants refused by a Judicial Commissioner.
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse the Secretary of State decision to issue (a) class and (b) specific BPD warrants.
- The number of (a) class and (b) specific BPD warrants issued by the Secretary of State and approved by a Judicial Commissioner.

- The number of times an urgent specific BPD warrant has been (a) submitted and (b) authorised by the Secretary of State and issued by a senior official.
- The number of times that the decision to authorise an urgent specific BPD warrant has subsequently been refused by a Judicial Commissioner.
- The number of renewals of (a) class and (b) specific BPD warrants that were made.
- The number of (a) class and (b) specific BPD warrants that were cancelled.
- The number of (a) class and (b) specific BPD warrants extant at the end of the calendar year.
- The number and details of modifications to add an operational purpose to the warrant, vary an operational purpose or remove an operational purpose from the warrant.
- The number and details of urgent modifications to add an operational purpose to the warrant or vary an operational purpose the warrant.
- The number and details of urgent modifications to add or vary an operational purpose (including on an urgent basis) where the decision was refused by a Judicial Commissioner.
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse to approve a decision to modify an urgent specific BPD warrant.
- A record of BPDs held that fall within a particular class warrant (see chapter 6 above)
- A record of any intentional examination of confidential information relating to sensitive professions (see paragraph 7.8 and subsequent paragraphs)
- A list of all BPD deleted or destroyed in the previous six months (see paragraph 7.20)

8.4 These records must be sent in written or electronic form to the Investigatory Powers Commissioner, as determined by the Commissioner. Guidance on record keeping may be issued by the Investigatory Powers Commissioner. Guidance may also be sought from the Commissioner by the Security and Intelligence Agencies.

8.5 The Investigatory Powers Commissioner will use this information to inform their oversight and, where appropriate, include in their report to the Prime Minister about the carrying-out of the functions of the Judicial Commissioners. The Prime Minister may, after consultation with the Investigatory Powers Commissioner, exclude from publication any part of the report if, in the opinion of the Prime Minister, the publication would be contrary to the public interest or prejudicial to national security, prevention or detection of serious crime, or the continued discharge of the functions of the overseen public authorities.

8.6 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 serious breaches of safeguards that have resulted in an unauthorised or unjustifiable interference with privacy, as agreed with the Investigatory Powers Commissioner, must be reported to the Commissioner. The Investigatory Powers Commissioner may issue guidance in respect of error-reporting which the Security and Intelligence Agency must have regard to.

9 Oversight

9.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ('the IPC'), whose remit includes providing comprehensive oversight of the retention, use or disclosure of bulk personal datasets by the security and intelligence agencies and adherence to the practices and processes described by this code. By statute the IPC will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The IPC will be supported by inspectors and others, such as technical experts, qualified to assist the IPC in their work.

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

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

9.4 Anyone working for a public authority or communications service provider who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner, who will consider them. In particular, any person who exercises the powers described in the Act or this code must, in accordance with the procedure set out in error reporting provisions of chapter 8 of the code, report to the Commissioner any action undertaken which they believe to be contrary to the provisions of this code. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority. The Commissioner may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the Investigatory Powers Tribunal (IPT).

9.5 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to an individual who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the individual affected. Further information on errors can be found in chapter 8 of this code. The public body who has committed the error will be able to make representations to the Commissioner before they make their decision on whether it is in the public interest for the individual to be informed.

9.6 The Commissioner must also inform the affected individual of their right to apply to the IPT (see chapter 10 for more information on how this can be

done) who will be able to fully investigate the error and decide if a remedy is appropriate. The IPC must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions for reasons of national security. Only the Prime Minister will be able to authorise redactions to the IPC's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

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

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

10 Complaints

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

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

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

The Investigatory Powers Tribunal

PO Box 33220

London

SWIH 9ZQ

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

11 Annex A

The Security Service Act 1989 and the Intelligence Services Act 1994

11.1 The **Security Service Act 1989** (SSA) provides that the functions of the Security Service are the protection of national security, the safeguarding of the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands and the provision of support to the police and other law enforcement authorities in the prevention and detection of serious crime.

11.2 The **Intelligence Services Act 1994** (ISA) sets out the functions of the Secret Intelligence Service (SIS) and Government Communications headquarters (GCHQ). In the case of SIS these are: obtaining and providing information relating to the actions or intentions of persons outside the British Islands; and performing other tasks relating to the actions or intentions of such persons. In the case of GCHQ these are: monitoring, making use of or interfering with communications and related equipment; and providing advice on information security and languages. ISA goes on to provide that their respective functions (with the exception of GCHQ's information security and language functions) may only be exercisable (a) in the interests of national security, with particular reference to the defence and foreign policies of the UK Government, (b) in the interests of the economic well-being of the UK, or (c) in support of the prevention or detection of serious crime.

11.3 The information gateway provisions in section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of ISA impose a duty on the Heads of the respective Agencies to ensure that there are arrangements for securing (i) that no information is obtained by the relevant Agency except so far as necessary for the proper discharge of its functions; and (ii) that no information is disclosed except so far as is necessary for those functions and purposes or for the additional limited purposes set out in section 2(2)(a) of ISA (in the interests of national security, for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings), section 4(2)(a) of ISA (for the purpose of any criminal proceedings) and section 2(2)(a) of SSA (for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings).

11.4 SSA and ISA accordingly impose specific statutory limits on the information that each of the Security and Intelligence Agencies can obtain, and on the information that each can disclose. These statutory limits do not simply apply to the obtaining and disclosing of information from or to other persons in the United Kingdom: they apply equally to obtaining and disclosing information from or to persons abroad.

The Counter-Terrorism Act 2008

11.5 Section 19 of the **Counter-Terrorism Act 2008** confirms that 'any person' may disclose information to the Agencies for the exercise of their respective functions, and disapplies any duty of confidence (or any other restriction, however imposed) which might otherwise prevent this. It further confirms that information obtained by any of the Security and Intelligence Agencies in connection with the exercise of any of its functions may be used by that Service in connection with the exercise of any of its other functions. For example, information that is obtained by the Security Service for national security purposes can subsequently be used by the Security Service to support the activities of the police in the prevention and detection of serious crime.

The Human Rights Act 1998

11.6 Each of the Security and Intelligence Agencies is a public authority for the purposes of the Human Rights Act 1998. When obtaining, using, retaining and disclosing bulk personal datasets, the Security and Intelligence Agencies must therefore (among other things) ensure that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. In practice, this means that any interference with privacy must be both necessary for the performance of a statutory function of the relevant Intelligence Agency and proportionate to the achievement of that objective.

The Data Protection Act 1998

11.7 Section 1(1) of the **Data Protection Act 1998** defines '*personal data*' as:

"data which relate to a living individual who can be identified –

- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of the data controller [i.e. in this case, the relevant Intelligence Service], and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

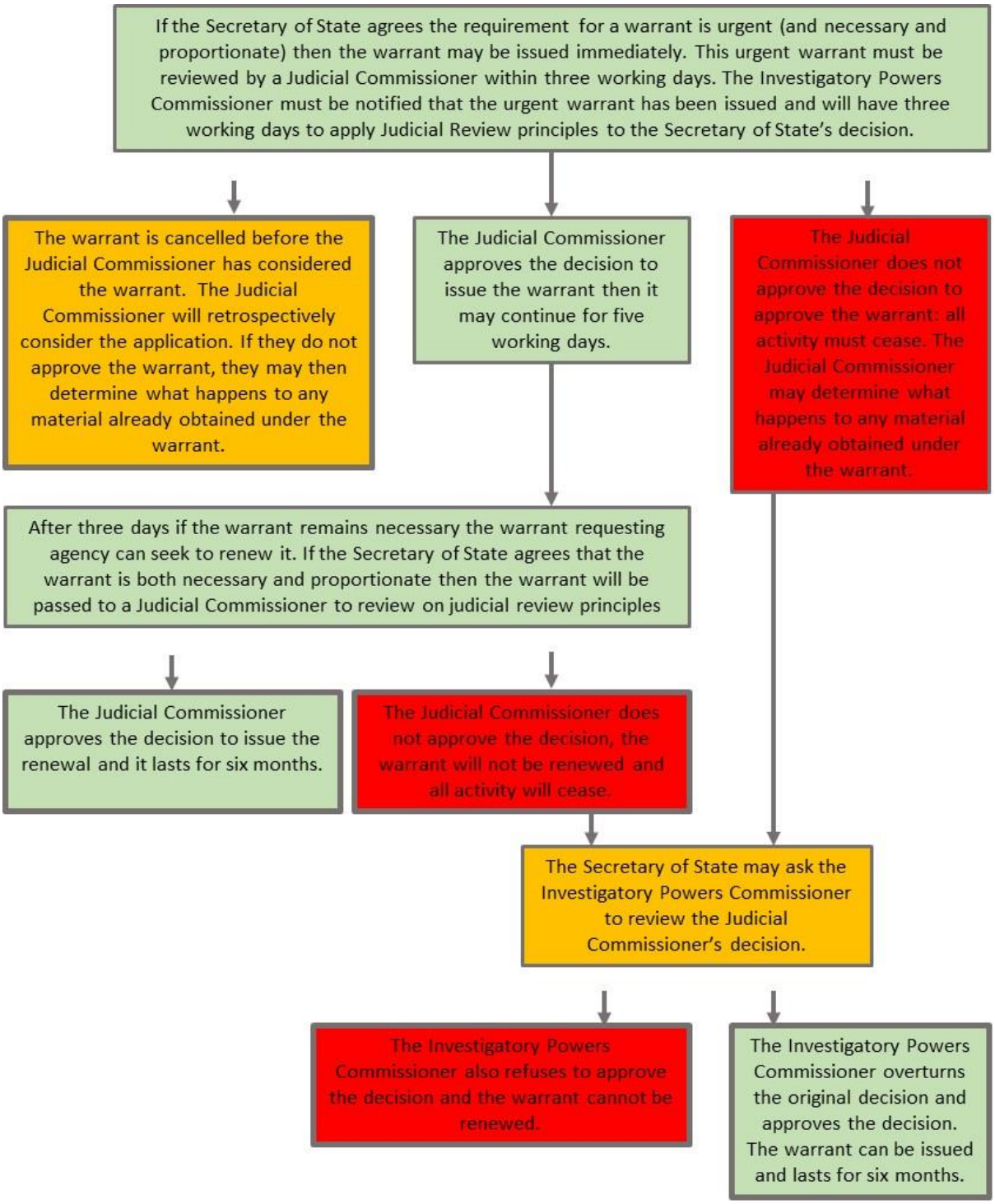
11.8 Section 2 of the DPA defines "sensitive personal data" as meaning personal data in relation to a data subject consisting of information as to the following:

- Racial or ethnic origin
- Political opinions
- Religious belief or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition

- Sexual life
- The commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

11.9 Each of the Security and Intelligence Agencies is a data controller in relation to all the personal data that it holds. Accordingly, when the Security and Intelligence Agencies use any bulk data that contain personal data, they must ensure that they comply with the Data Protection Act 1998 (except in cases where exemption under section 28 is required for the purpose of safeguarding national security).

12 Annex B


If the Secretary of State agrees the requirement for a warrant is urgent (and necessary and proportionate) then the warrant may be issued immediately. This urgent warrant must be reviewed by a Judicial Commissioner within three working days. The Investigatory Powers Commissioner must be notified that the urgent warrant has been issued and will have three working days to apply Judicial Review principles to the Secretary of State's decision.
The warrant is cancelled before the Judicial Commissioner has considered the warrant. The Judicial Commissioner will retrospectively consider the application. If they do not approve the warrant, they may then determine what happens to any material already obtained under the warrant.
The Judicial Commissioner approves the decision to issue the warrant then it may continue for five working days.
The Judicial Commissioner does not approve the decision to approve the warrant: all activity must cease. The Judicial Commissioner may determine what happens to any material already obtained under the warrant.
After three days if the warrant remains necessary the warrant requesting agency can seek to renew it. If the Secretary of State agrees that the warrant is both necessary and proportionate then the warrant will be passed to a Judicial Commissioner to review on judicial review principles
The Judicial Commissioner approves the decision to issue the renewal and it lasts for six months.
The Judicial Commissioner does not approve the decision, the warrant will not be renewed and all activity will cease.
The Secretary of State may ask the Investigatory Powers Commissioner to review the Judicial Commissioner's decision.
The Investigatory Powers Commissioner also refuses to approve the decision and the warrant cannot be renewed.
The Investigatory Powers Commissioner overturns the original decision and approves the decision. The warrant can be issued and lasts for six months.

13 Annex C

The text in this annex is intended to provide an indication of the additional safeguards that would be added to the BPD code of practice if amendments to Part 7 of the Bill relating to protected data and legal professional privilege (LPP) are passed by the House of Lords at Report. The text does not aim to reflect a definitive list of all other related amendments (to for example, LPP) that may be made to other Parts of the Bill at Report and read across to Part 7 – and so necessitate further changes to all the associated codes of practice.

BPD warrant applications

Extra bullet to be added to list at paragraph 4.13 of draft code – 'In the 'Case 2' scenario…' – as the first bullet. NB in the introductory text above the bullets, the word 'two' will need to be changed to 'three':

- If the Agency considers that the BPD contains any **protected data** (see paragraph xxx and subsequent paragraphs).

Footnote to be added to the last bullet of paragraph 4.13. The footnote would read:

'See paragraph 4.xx and paragraph 7.yy for specific safeguards in respect of legal professional privilege (LPP). In practice, LPP will only arise in the case of 'protected data', and so a BPD containing LPP will in any event be caught by the specific provisions in the Bill on such data: namely, a statutory prohibition on the use of class warrants and requirement to apply for a specific warrant, coupled with a power for the Secretary of State to attach conditions where 'UK content' is selected for examination, and specific access controls for intended/expected selection for examination of LPP.'

The following text is to be inserted at the end of chapter 4 of the BPD code of practice:

BPDs containing 'protected data' – further restriction on class warrants and provision for attaching conditions to specific warrants

Introduction

13.1 Part 7 does not regulate a technique for acquiring information, but rather a species of data that may be acquired from a variety of different sources and by different methods, as set out in Chapter 2 of this Code. This fact means that, to the extent that the retention and examination of BPDs may be

regarded as a capability, it is one that is of a different nature and kind from the techniques of bulk interception and bulk equipment interference.

13.2 Where data are acquired via bulk interception or bulk equipment interference, the degree of intrusiveness of the data falling into the protected class will depend on the nature and variety of the communications or items of information that are obtained from the systems or equipment in issue. It may therefore be difficult for the Agency implementing the warrant to assess in advance the nature and intrusiveness of all the data falling into the protected class that may be obtained by means of the bulk warrant. The Act must therefore apply the most stringent access controls to the selection for examination of all protected material relating to an individual known to be in the British Islands at the time of the selection. The statutory framework governing bulk interception and bulk equipment interference accordingly requires an Agency to obtain a targeted examination warrant when selecting for examination any protected material obtained under the warrant relating to an individual known to be in the British Islands at the time of the selection.

13.3 By contrast, where an Agency obtains a set of information other than in exercise of a power conferred by the Act, the Agency must conduct an initial examination to determine whether the set of information constitutes a BPD. If the set of information is retained as a BPD, the Agency will therefore be better able to assess the nature and intrusiveness of any data in the dataset that fall into the protected class. In particular, the Agency should be able to identify any protected data that comprise the contents of e-mails, letters or other documents. It will accordingly be possible for the Secretary of State and the Judicial Commissioner, at the time a specific BPD warrant is issued, and having regard to the Agency's initial examination and assessment, to determine the safeguards that should apply to the selection for examination of protected data relating to an individual known to be in the British Islands up to, and including, a requirement to obtain the prior written approval of the Secretary of State and the Judicial Commissioner.

13.4 The stringent selection for examination safeguards in section 202 of the Act will already be sufficient to regulate the vast majority of cases where data contained in a BPD is selected for examination. These safeguards ensure that any selection for examination of data contained in a BPD is carried out only for the operational purposes specified in the warrant (which have been approved by the Secretary of State and Judicial Commissioner "double lock"). In addition, the selection of any such data for examination must be necessary and proportionate in all the circumstances.

13.5 Given the range and variation in intrusiveness of protected data (as defined in the annex to this Code) contained in BPDs, it is not necessary or appropriate to apply additional controls to the selection for examination of all protected data in BPDs relating to an individual known to be in the British Islands at the time of the selection. Nor is it feasible for the Act to seek to identify all the various types of protected data that may be contained in BPDs, or to provide in detail for the limitations on access to each type of field depending on its relative intrusiveness, over and above those already mandated in section 202.

13.6 This Chapter of the Code accordingly sets out a scheme that enables the Secretary of State (with the approval of the Judicial Commissioner) to impose

additional controls in relation to the selection for examination of any protected data in the dataset relating to individual is known to be in the British Islands at the time of the selection. The scheme applies on a dataset by dataset basis having regard to the range of factors set out below, including the nature and intrusiveness of the protected data in the dataset.

Categorising data in BPD

13.7 For the purposes of this scheme, "protected data" has the meaning prescribed by section xxx of the Act and set out in this Code.

13.8 When categorising data contained in a BPD, the Agencies should first consider whether the dataset as a whole comprises data that are not "private information" (see paragraph 13.13). For example, a dataset consisting of data that are freely available online and are not subject to any privacy settings or access controls should be categorised as non-private information. No data fields in non-private datasets are protected data for the purposes of Part 7.

13.9 Except where paragraph 13.8 applies, the Agency should approach categorisation by determining whether the data contained in the BPD are systems data or identifying data (or both) and, if not, whether the data are not private information. These definitions are explained further below. Data that are systems data, identifying data or non-private are not protected. In cases where the Agency's initial examination of the BPD suggests that data within the dataset are the contents of letters, e-mails or other documents, then the Agency should assume that the BPD contains protected data (though that does not mean that all the data contained in that BPD are protected).

13.10 **Identifying data** in a BPD is data that may help to identify persons, systems services, locations or events. Identifying data in a BPD does not therefore, of itself, need to identify a person etc. For example, a person's name, address, occupation and country of birth in a BPD will all be identifying data, even though any one of them, on its own, might not identify that person etc. The majority of non-protected data in a BPD are likely to be categorised as identifying data.

13.11 **Systems data** is any data that enables or facilitates the functioning of any system or service. It includes all data that a system requires to function and provide its services. For example, if a passport number in a flight booking system has to be valid for the passenger to be able to fly then that passport number, when included in a travel BPD, will be systems data. The passport number will also be BPD identifying data.

13.12 Where a data field is correctly classified as systems data because the operation of the system or service is dependent on the validity of the value of that field, the data field should be permanently categorised as systems data. That remains the case even if the dataset containing the systems data field is passed to a third party and is retained on a different system.

13.13 **Private information** includes information relating to a person's private or family life. In the BPD context, information falling which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, web forums, online social networking, mapping imagery, commercial subscription databases, academic articles, conference proceedings, business reports, and more. Such

information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

13.14 **Protected data** in relation to a BPD is any data contained in a BPD other than data which is one or more of the following: (a) identifying data (see paragraphs 13.10 and 13.15), (b) systems data, or (c) data which is not private information (see sections xx and 239(2) to 239(4) of the Act).

13.15 Protected data may contain embedded data items that individually:

- fall within the definition of identifying data (see section 239(2) to 239(3));
- are capable of being logically separated from the BPD or the other data in the BPD; and
- if they were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the BPD or that other data , disregarding any meaning arising from the existence of the BPD or the other data or from any data relating to that fact.

13.16 If an individual data item meets these conditions then it should be categorised as identifying data in its own right – whilst the categorisation of the protected data from which it was derived remains unaffected.

Requirement to apply for a specific warrant for BPDs containing protected data

13.17 Where, to the best of the relevant Security and Intelligence Agency's knowledge or belief (and having regard to paragraph 13.7 above), it considers it likely that a BPD contains any protected data, it must apply for a specific warrant.

13.18 As required by section 188, the application for a specific BPD warrant in such a case must include:

- a description of the specific dataset to which the application relates; and
- the "operational purposes" for which the relevant Security and Intelligence Agency wishes to examine the BPD.

Additional range of factors to be included in the specific BPD warrant application

13.19 In addition, the warrant application in a case falling within paragraph 13.17 above should also contain as much information, and be as specific as is practically possible, in relation to the protected data in the BPD, including **the nature and type of the data and any other factors that may be relevant when assessing the level of intrusiveness of the protected data**. This is with a view to ensuring that the Secretary of State can:

- assess whether the safeguards in section 202 are adequate and sufficient for the selection for examination of protected data in the dataset relating to an individual known to be in the British Islands at the time of the selection; and

- if the safeguards in section 202 are not sufficient, attach conditions to the warrant in accordance with section xx of the Act.

13.20 In particular, without prejudice to the generality of the foregoing, the application for a specific warrant in such a case should include (so far as reasonably practicable) the following specific information:

- a description of the structure and scope of the dataset and of the information contained within it, including the different data involved and the nature and categories of data captured in those data, and, in particular, whether those data are legally privileged[2];
- a description, to include as much detail as is practically possible, of the nature and extent of the data which, following the relevant Agency's initial examination of the dataset, it is known or believed may contain protected data;
- whether any of the protected data are the contents of e-mails, letters or other documents;
- whether any of the protected data contain communications between a member of a relevant legislature (as defined in sections 26 and 106) and another person on constituency matters or other parliamentary business;
- any other factors that may be relevant to the Secretary of State's assessment of the level of intrusiveness of the protected data in the BPD (and therefore of the adequacy of the section 202 safeguards), including the extent of the expectation of privacy arising from the circumstances and context in which the protected data were included in the BPD;
- the Agency's assessment of whether, having regard to the above factors, the specific warrant should be issued unconditionally or only subject to such conditions as may be approved by the Secretary of State.

Authorising specific warrants for BPDs containing protected data

13.21 When considering a warrant application for any dataset falling within paragraph 13.17 above, the Secretary of State must determine, in the light of the **range of factors** set out in paragraphs 13.19 and 13.20 above, whether the Secretary of State is satisfied that the selection for examination safeguards set out in section 202 would be adequate and sufficient for the selection for examination of the protected data in the dataset relating to an individual known to be in the British Islands at the time of the selection. The section 202 safeguards are likely to be adequate and sufficient to provide the necessary Article 8 protections in cases where the BPD comprises a dataset containing a relatively small number of protected data of a low level of intrusiveness (for example, protected data contained in a travel BPD provided by a prospective traveller to a service provider or in an internet dataset with minimal privacy settings which is accessible by a very large user group).

13.22 Where the Secretary of State is so satisfied, the Secretary of State may issue the warrant without conditions.

[2] The additional safeguards that apply when a Security and Intelligence Agency wishes to select for examination legally protected fields are set out in Chapter 7 of this Code.

13.23 Where the Secretary of State is not so satisfied, but would otherwise be minded to issue the warrant (subject to the approval of the Judicial Commissioner), the Secretary of State may by virtue of the power conferred by section xxx of the Act **attach conditions** to the issue of the warrant in the way set out in paragraphs 13.24 to 13.27 below. In cases where the dataset contains the contents of letters, e-mails and documents, the Secretary of State will ordinarily require the Agency to obtain the prior written approval of the Secretary of State and the Judicial Commissioner.

Conditions which may be attached to the warrant in the exercise of the Secretary of State's discretion

13.24 In cases falling within paragraph 13.21 above, pursuant to the power conferred by section xxx of the Act, the Secretary of State may attach conditions to the issue of the warrant, in the exercise of the Secretary of State's discretion, up to, and including, a requirement to obtain the prior written approval of the Secretary of State and the Judicial Commissioner when:

- the relevant Agency wishes to select for examination any protected data contained in the BPD using criteria referable to an individual known to be in the British Islands at that time, and
- the purpose of using those criteria is to identify protected data relating to that individual.

13.25 The conditions that may be attached to the warrant by the Secretary of State in accordance with paragraph 13.24 may also include (as an alternative to the requirement referred to in paragraph 13.24) such requirement or requirements as the relevant Security and Intelligence Agency may suggest and which the Secretary of State agrees are appropriate. These may include – but are not limited to – one or more of the following requirements:

- to seek the prior approval of a senior manager in the relevant Security and Intelligence Agency and, if the Secretary of State considers appropriate, subject to the condition that the senior manager in question is independent of the investigation, operation or analytic work to which the selection for examination relates;
- to seek the prior approval of a senior official in the Secretary of State's Department; or
- a prohibition on selecting for examination any protected fields in the BPD using criteria referable to an individual known to be in the British Islands at the time of the selection (and a determination, on that basis, that the section 202 safeguards are adequate and sufficient).

13.26 Where the dataset contains protected data of differing levels of intrusiveness, and the Secretary of State considers that only some of those data require the additional controls, the Secretary of State may choose either (a) to apply the additional controls only to those data which require the additional controls or (b) to apply the additional controls to all the protected data contained in the dataset.

13.27 An approval for the purposes of paragraph 13.24 or paragraph 13.25 need not relate to a particular person or organisation. For example, an authorisation may cover a group who share a common purpose or who are carrying on a particular activity, or may relate to more than person where the authorisation is given for the purposes of a single operation or investigation.

Renewals of specific BPD warrants issued unconditionally

13.28 When applying for **the renewal of a specific BPD warrant** issued without conditions, the relevant Security and Intelligence Agency should report to the Secretary of State on the extent to which any protected data in the dataset have, since the issue or last renewal of the warrant, been selected for examination using criteria referable to an individual known to be in the British Islands at that time.

13.29 In cases where the Secretary of State is minded to renew such a warrant, the Secretary of State may either (a) renew the specific BPD warrant, or (b) approve the retention of the BPD as part of a class BPD warrant. Each time such a class BPD warrant is subsequently renewed, the relevant Security and Intelligence Agency should, so far as is reasonably practicable, report to the Secretary of State on the frequency with which protected data in the dataset has, since the issue or last renewal of the warrant, been selected for examination using criteria referable to an individual known to be in the British Islands at that time.

BPDs containing unanticipated protected data

13.30 It is possible that cases may occasionally arise where an agency discovers, following the selection for examination of data contained in a BPD retained pursuance to a BPD warrant, that the BPD contains protected data fields which were not identified as protected at the time of the initial examination or where there was an urgent need to issue the warrant. Where such cases arise, the Agency must apply for a specific BPD warrant as soon as possible in accordance with the procedure set out at paragraphs 13.17 to 13.27. The Agency must also ensure, as soon as reasonably practicable, that any selection for examination of the protected data in the BPD using criteria referable to an individual known to be in the British Islands ceases, until such time as the specific BPD warrant has been issued.

Safeguards

New sentence to be added to the end of paragraph 7.9:

13.31 The Agencies should also ensure that SIA staff, when undertaking such searches, comply with the additional safeguards set out below relating to Members of Parliament, legally privileged material and journalistic material.

For insertion after the section in chapter 7 titled 'Additional access safeguards for confidential information relating to sensitive professions':

Selection for examination of protected data relating to a Member of Parliament

13.32 These paragraphs apply where:

- A Security and Intelligence Agency wishes to search a BPD retained pursuant to a specific BPD warrant and the purpose of the search is to select for examination protected data relating to a member of a relevant legislature; and
- the specific warrant has been issued subject to a requirement to obtain the prior written approval of the Secretary of State and the Judicial Commissioner.

13.33 Where these paragraphs apply, the Agency must have obtained the prior approval of the Prime Minister to target the member of the legislature. Prior approval must be obtained regardless of whether the member of the relevant legislature is inside or outside the British Islands at the time of the selection for examination.

13.34 "Member of a relevant legislature" for these purposes has the meaning given in sections 26 and 106 of the Act.

Material subject to legal privilege

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

13.36 Legal privilege does not apply to material held with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged material will lose its protection if, for example, the professional legal adviser is intending to hold or use the material 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.

13.37 For the purposes of this Code, any communication between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the items do not form part of a professional consultation of the lawyer, or there is clear and compelling evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the material is subject to legal privilege or over whether the material is 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 Security and Intelligence Agency.

13.38 Selecting legally privileged protected material for examination 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 selection for examination of legally privileged protected data contained in BPDs (whether deliberately or otherwise) is therefore subject to the additional safeguards set out in paragraph 13.39 and subsequent paragraphs of this Code. The guidance set out may in part depend on whether the legally privileged protected data have been selected intentionally or incidentally to other data which have been sought.

Selection of legally privileged protected fields for examination

13.39 These paragraphs apply where a Security and Intelligence Agency wishes to search a BPD and:

- the purpose, or one of the purposes of the search, is to select for examination protected data subject to legal privilege, or
- the use of the relevant search criteria is likely to identify such data.

13.40 Where these paragraphs apply (and without prejudice to Chapter 4 of this Code), the Agency is prohibited from carrying out the search unless prior approval has been given by a relevant approver. The relevant approver in the case of a search relating to an individual known to be in the British Islands at the time of the selection is the Secretary of State, subject to the approval of the Judicial Commissioner. In any other case, the relevant approver is a senior official (who must not be a member of the Security and Intelligence Agencies).

13.41 Before carrying out the search, the Agency must notify the relevant approver. Where the use of the search criteria is likely to identify legally privileged protected data, the notification to the senior official should include, in addition to the reasons why it is considered necessary for the selection for examination to take place, an assessment of how likely it is that legally privileged protected data will be selected. In addition, the notification should state whether the purpose, or one of the purposes of the search, is to select

for examination legally privileged protected data. Where the intention is not to identify legally privileged protected data, but it is likely that such data will nevertheless be selected, that should be made clear in the notification, and the Agency should confirm that any inadvertently obtained privileged data 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 those data.

13.42 On receiving the notification, the relevant approver must decide whether to give an approval for the search to be carried out. The relevant approver may give an approval only if:

- the approver considers that the arrangements made for the purposes of section 188(6)(d) include specific arrangements for the handling, retention, use and destruction of legally privileged protected data, and
- where the first bullet of paragraph 13.39 applies, the approver considers that there are exceptional and compelling circumstances that make it necessary to authorise the search. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb or in the interests of national security, and the selection for examination is reasonably regarded as likely to yield intelligence necessary to counter the threat.

13.43 In the event that legally privileged protected data are inadvertently and unexpectedly selected for examination (and where the enhanced procedure set out above has consequently not been followed), any protected data so obtained must be handled strictly in accordance with the provisions of this chapter. No further privileged protected data may be intentionally selected for examination by reference to the relevant search criteria unless approved by the relevant approver as set out in paragraph 13.42.

Handling, retention and deletion

13.44 Officials who examine protected data contained in BPDs should be alert to any data which may be subject to legal privilege.

13.45 Where it is discovered that legally privileged protected data have been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain them. If not, the protected data should be securely destroyed as soon as possible.

13.46 Where protected data have been identified following examination as legally privileged, and are recorded and retained separately from the bulk personal dataset for purposes other than their destruction they should be clearly marked as subject to legal privilege. Such data should be retained only where it is necessary and proportionate to do so. It must be securely destroyed when its retention is no longer needed for the authorised statutory purposes. If such data are retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for those purposes.

Dissemination

13.47 Protected data 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.

13.48 The dissemination of legally privileged protected data 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 legally privileged protected data 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 legally privileged protected data in order to gain a litigation advantage over another party in legal proceedings.

13.49 In order to safeguard against any risk of prejudice or accusation of abuse of process, public authorities must also take all reasonable steps to ensure that lawyers or policy officials with conduct of legal proceedings should not see legally privileged protected data 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 content could yield a litigation advantage, the direction of the Court must be sought.

Reporting to the Commissioner

13.50 In those cases where legally privileged protected data following their examination are recorded and retained separately from the bulk personal dataset for purposes other than their destruction, the relevant Agency must inform the Investigatory Powers Commissioner as soon as is reasonably practicable, as agreed with the Commissioner. Any legally privileged protected data that are still being retained should be made available to the Commissioner on request, including detail of whether those data have been disseminated.

Selection for examination of confidential journalistic protected data

13.51 Confidential journalistic protected data are data in a BPD that contain data acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

13.52 Where the intention is to select for examination confidential journalistic protected data, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the selection for examination of confidential journalistic protected data 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 Security and Intelligence Agency.

13.53 Confidential journalistic protected data which have been identified as such should be retained only where it is necessary and proportionate to do so for. It must be securely destroyed when its retention is no longer needed for those purposes. If such data are retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate.

13.54 Where confidential journalistic protected data have been identified in a bulk personal dataset following their examination, they should be retained only where it is necessary and proportionate to do so. In those cases were such data are recorded and retained separately from the dataset for purposes other than their destruction or are disseminated to an outside body, all reasonable steps should be taken to protect the confidentiality of the data. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential journalistic protected data, advice should be sought from a legal adviser within the Security and Intelligence Agency and before any further dissemination of the content takes place.

13.55 In any case where confidential journalistic protected data following their examination are recorded and retained separately from the bulk personal dataset for purposes other than their destruction, the relevant agency must inform the Investigatory Powers Commissioner as soon as is reasonably practicable, as agreed with the Commissioner. Any data which has been retained should be made available to the Commissioner on request.

Home Office

Equipment Interference

DRAFT Code of Practice

Autumn 2016

Equipment Interference

DRAFT Code of Practice

Pursuant to Schedule 7 to the Investigatory Powers Act 2016

Autumn 2016

Contents

1 Introduction

Background

1.1 This code of practice provides guidance on the use by the Security and Intelligence Agencies (Security Service, Secret Intelligence Service ("SIS"), and Government Communications Head Quarters ("GCHQ"), law enforcement agencies and Defence Intelligence ("the equipment interference agencies") of the Investigatory Powers Act 2016 ("the Act") to authorise equipment interference. It provides guidance on when a warrant under the Act is required to carry out equipment interference, the procedures that must be followed before equipment interference can be carried out, and on the examination, retention, destruction and disclosure of any information obtained by means of the interference.

1.2 The Act provides a statutory framework for authorising equipment interference when the European Convention of Human Rights ("the ECHR") and/or the Computer Misuse Act 1990 ("the CMA") are likely to be engaged. Chapter 2 of the code provide further guidance on the CMA, and when equipment interference warrants are required under the Act.

1.3 This code is issued pursuant to Schedule 7 of the Act, which provides that the Secretary of State shall issue one or more codes of practice about the exercise of functions conferred by virtue of the Act. This code replaces the previous equipment interference code of practice issued in 2015 which governed the Security and Intelligence Agencies' use of equipment interference.

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

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

Effect of code

1.6 Paragraph 6 of Schedule 7 to the Act provides that all codes of practice issued under the Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal ("the IPT") established under the Regulation of Investigatory Powers Act 2000 ("RIPA"), or to a supervisory authority[1] exercising functions under the Act, it must be taken into account. The equipment interference agencies may also be required to justify, with regard to this code, the use of equipment interference warrants in general or the failure to use warrants where appropriate.

[1] A supervisory authority is the IPC or any other Judicial Commissioner: see paragraph 6 of Schedule 7 to the Act.

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

Equipment interference to which this code applies

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

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

1.10 An equipment interference warrant provides lawful authority to carry out the acquisition of communications stored in or by a telecommunications system. Where equipment interference activity amounts to interception of the content of communications in the course of their transmission (for example, live interception of an online video call), an interception warrant must be obtained under Part 2 or Chapter 1 of Part 6 of the Act.

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

Basis for lawful equipment interference activity

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

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

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

[2] Including equipment.

1.15 Part 5 and Chapter 3 of Part 6 of the Act provide a statutory framework under which equipment interference activities which engage the ECHR and/or would otherwise constitute an offence under the CMA can be authorised and conducted lawfully. The use of equipment interference warrants is mandatory in certain circumstances by virtue of section 11 of the Act and this code. Equipment interference agencies may choose to authorise equipment interference under the Act in other circumstances, but are not required to do so. Conduct which has lawful authority by virtue of an equipment interference warrant is treated as lawful for all other purposes.

2 Scope and definitions

Overview

2.1 Equipment interference warrants authorise interference with equipment for the purpose of obtaining communications, equipment data or other information and any conduct required to carry out authorised interference.

2.2 This chapter provides further guidance on the scope of equipment interference and relevant definitions, and on the circumstances where an equipment interference warrant is required for an equipment interference agency to undertake equipment interference activity.

Equipment interference

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

2.4 Equipment interference can be carried out either remotely or by physically interacting with the equipment. Equipment interference operations vary in complexity. At the lower end of the scale, an equipment interference agency may covertly download data from a subject's mobile device when it is left unattended, or an agency may use someone's login credentials to gain access to data held on a computer. More complex equipment interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device.

Example 1: An equipment interference agency covertly downloads data from a device (such as a smart phone or laptop) either through direct access to the device itself (for example by access to USB ports) or by remotely installing software which enables material to be extracted.

Example 2: Key logging software is installed on a device by an equipment interference agency, making it possible to track every keystroke entered by users. The agency uses the key logger to track the keystrokes used when logging into a relevant website.

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

2.6 Interference with equipment that is not for the purpose of acquiring communications, equipment data or other information will continue to fall within the definition of 'property interference' for the purposes of the Covert Surveillance and Property Interference Code of Practice. For example, disabling an alarm system to allow covert access to a building does not constitute equipment interference, although it may be necessary to interfere with the alarm system (equipment) to acquire equipment data in order to understand the operating system of the alarm system to enable it to be disabled. In such circumstances, the purpose of the interference is to defeat the alarm system and the acquisition of the equipment data is incidental. To the extent such activities would otherwise be unlawful, it should continue to be authorised under section 5 or 7 of Intelligence Services Act 1994 ("the 1994 Act") or Part 3 of the Police Act 1997 ("the 1997 Act").

2.7 This distinction has been drawn so that the Act can apply tailored safeguards, handling arrangements and oversight to activity where the purpose of the interference is to acquire communications, equipment data or other information from equipment. Different considerations will apply where the purpose of the interference is not to obtain communications, equipment data or other information, accordingly, the safeguards required differ to those applicable to equipment interference under the Act, and are provided through existing legislation.

Equipment

2.8 Equipment is defined in sections 127 and 182 of the Act. “Equipment" comprises any equipment producing “electromagnetic, acoustic or other emissions” and any device capable of being used in connection with such equipment. "Equipment" for these purposes is not limited to equipment which is switched on and/or is emitting signals but also includes equipment which is capable of producing such emissions.

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

2.10 Equipment to which this code applies will vary as new technology is developed and produced. When reviewing this code of practice the Investigatory Powers Commissioner (“IPC”) should give particular consideration to this definition.

Equipment data

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

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

2.12 Equipment data is defined in sections 95 and 164 of the Act. Equipment data includes:

- Systems data:
  - Systems data includes two types of data. It includes the data which (when a communication is transmitted via a telecommunications system) is comprised in, attached to or logically associated with that communication and is necessary for the telecommunication system to transmit the communication. Second, there is other data comprised in, attached to or logically associated with communications or items of information which enable systems or services to function. While this second type of systems data is not necessary for a transmission system to transmit

a communication, it is also not content. These two types of data make up the broader set of information which is called systems data[3].

- Examples of systems data would be:
  - messages sent between items of network infrastructure to enable the system to manage the flow of communications;
  - router configurations or firewall configurations;
  - software operating system (version);
  - historical contacts from sources such as instant messenger applications or web forums;
  - alternative account identifiers such as email addresses or user IDs; and
  - the period of time a router has been active on a network.

- Identifying data:
  - A communication or item of information may include data which may:
  - be used to identify, or assist in identifying, any person, apparatus, system or service;
  - be used to identify any event; or
  - be used to identify the location of any person, event or thing.
  - In most cases this data will be systems data, however, there will be cases where this information does not enable or otherwise facilitate the functioning of a service or system and therefore is not systems data. Where such data, can be logically separated from the remainder of the communication or item of information and does not, once separated, reveal anything of what might reasonably be considered to be the meaning (if any) of any communication or item of information (disregarding any inferred meaning) it is identifying data.

- Examples of such data include:
  - the location of a meeting in a calendar appointment;
  - photograph information - such as the time/date and location it was taken; and
  - contact 'mailto' addresses within a webpage

Protected material

2.13 Protected material refers to material that is subject to particular access safeguards when acquired through bulk equipment interference and selected for examination using criteria referable to an individual known to be in the British Islands.

2.14 Protected material includes private information and the content of communications. Equipment data and non-private information (that is not a communication) are not protected material[4].

[3] Systems data that is necessary for the provision and operation of a service or system also includes the data necessary for the storage of communications and other information on relevant systems. Systems data held on a relevant system may be obtained via an equipment interference warrant under Part 5 or Chapter 3 of Part 6 of the Act.

[4] See section 179(9) of the Act.

Example: In the case of an email stored on a mobile phone, the message in the body of the email and the text in the subject line would not be equipment data (unless separated as identifying data). Accordingly, in the context of bulk equipment interference, this would be protected material and subject to the relevant safeguards set out in the Act when selected for examination using criteria referable to an individual known to be in the British Islands [5]*. Information associated with the stored email, such as the sender and recipient of the email or information about where the email is stored on the device, is equipment data and is not therefore protected material. In addition, information that is not private information which may be attached to the email, such as a publicly disseminated electronic magazine, would not be protected material*

Overseas-related communications, information and equipment data

2.15 Overseas-related communications, overseas-related information and overseas-related equipment data are defined in section 163 of the Act. The purpose of the definitions is to ensure that bulk equipment interference warrants are foreign focussed and are aimed at identifying communications and other information relating to individuals and entities outside the British Islands. The Security and Intelligence Agencies must accordingly ensure that the purpose of bulk equipment interference warrants is to obtain the communications, equipment data or other information of individuals or entities outside the British Islands.

Communications service provider

2.16 The obligations under Part 5 and Part 6 chapter 3 of the Act apply to telecommunications operators. Throughout this code, communications service provider ("CSP") is used to refer to a telecommunications operator.

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

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

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

[5] See section 179(9) of the Act.

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

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

Restrictions on interference with equipment

Computer Misuse Act 1990

2.22 Interfering with the functions of a computer and accessing its data or its programs, where there is no lawful authority to do so, may in certain circumstances amount to a criminal offence. Sections 13 and 14 of the Act impose restrictions on equipment interference agencies, where it is considered that the proposed conduct would constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990 (CMA). Accordingly, it is important that equipment interference agencies understand when a CMA offence is likely to be committed.

2.23 "Computer" is not defined in the CMA; rather the Act relies on the ordinary meaning of the word in the relevant context. Some guidance is provided by section 69 of the Police and Criminal Evidence Act 1984, where the term was held to mean "a device for storing, processing and retrieving information". Such devices fall within the definition of "equipment" in sections 127 and 182 of the Act.

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

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

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

Mandatory use of targeted and bulk equipment interference warrants: security and intelligence agencies

2.26 Section 13 of the Act provides that it is mandatory for a security and intelligence agency to obtain an equipment interference warrant for the purpose of obtaining communications, equipment data or other information where a CMA offence would otherwise be committed and there is a British Islands connection.

2.27 A British Islands connection exists if:

- any of the conduct would take place in the British Islands (regardless of the location of the equipment which would, or may be, interfered with),
- the intelligence service believes that any of the equipment would, or may, be in the British Islands at some time while the interference is taking place, or
- a purpose of the interference is to obtain:
  - communications sent by, or to, a person who is, or is believed to be in the British Islands;
  - private information relating a person who is, or is believed to be in the British Islands; or
  - Equipment data which forms part of, or is connected with, the communications or private information outlined above.

Example: A member of an equipment interference agency installs a piece of software on a device located outside the British Islands by means of conduct effected within the UK. The software sends back information about the activities of the user of the target device. The service must obtain a targeted equipment interference warrant as the conduct would otherwise amount to unauthorised access to computer material contrary to the CMA and there is a British Islands connection by virtue of where the conduct takes place.

2.28 It is not mandatory under the Act for a security and intelligence agency to obtain a bulk equipment interference warrant other than when a CMA offence is committed and there is a British Islands connection. As a matter of policy, however, and without prejudice as to arguments regarding the applicability of the ECHR, when a security and intelligence agency plans to engage in activity for which it is able to obtain a bulk equipment interference warrant it should do so. The difference between targeted and bulk equipment interference is explained in paragraph 5.5.

2.29 In no circumstances may an equipment interference agency seek to circumvent the requirement to obtain a warrant by asking an international partner to undertake equipment interference on its behalf.

Restrictions on interference for law enforcement agencies

2.30 The Act provides a statutory framework under which law enforcement agencies may authorise targeted equipment interference to which the Act applies. Whether a targeted equipment interference warrant is available or required will depend on a number of factors, including whether the CMA is engaged, the appropriate law enforcement officer making the application, the nature of the equipment interference, where the interference is taking place and where the conduct takes place from.

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

2.32 Accordingly, law enforcement officers will apply for an equipment interference warrant under this Act where the CMA is engaged and the conduct cannot be authorised under another law enforcement power. The CMA provides that access will not be ‘unauthorised’ if the conduct in question takes place pursuant to relevant authorisation.

Example: A law enforcement officer interferes with equipment by seizing it under powers arising from the Police and Criminal Evidence Act 1984 as relevant evidence in a criminal investigation. The officer's conduct is authorised by the 1984 Act and no equipment interference warrant is therefore required.

2.33 A law enforcement officer who is a member of a police force, the Ministry of Defence Police, the Police Investigations and Review Commissioner, the Independent Police Complaints Commission, the British Transport Police or the Police Services of Scotland or Northern Ireland may only be issued with a targeted equipment interference warrant if there is a British Islands connection (for definition of 'British Islands Connection' refer to paragraph 2.28). To further ensure that equipment interference activities conducted by these forces are focussed on investigations or operations within the British Islands, irrespective of whether there is a British Islands connection, these forces are prohibited by this code from obtaining an equipment interference warrant for interferences that takes place outside of the British Islands unless the subject of investigation is a UK national or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court. For example, such circumstances may arise where material is being acquired from equipment in the British Islands, but the equipment is subsequently temporarily taken outside the British Islands and the material continues to be captured[6].

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

2.34 Law enforcement agencies other than those set out in 2.34 of this code may be issued with targeted equipment interference warrants regardless of whether there is a British Islands connection. Officers in these forces may therefore undertake equipment interference activities outside the British Islands. This division reflects the different work that the agencies are expected to carry out. For example, the National Crime Agency, ("NCA") may investigate crimes that originate outside of the British Islands but impact upon the UK. Conversely, a regional police force would be unlikely to routinely investigate crimes outside of the UK. In practice, should a regional police force need to investigate crimes taking place where there is no British Islands connection they will do so with the assistance of another agency, such as the NCA.

Non-mandatory use of targeted equipment interference warrants

Security and intelligence agencies

2.35 By virtue of the Act and this code, it is not mandatory for a security and intelligence agency to obtain an equipment interference warrant in two circumstances.

2.36 Firstly, a security and intelligence agency need not obtain an equipment interference warrant where there is a British Islands connection, but the conduct to be authorised does not constitute an offence under the CMA. An agency may obtain an equipment interference warrant in these circumstances, but need not do so if another authorisation route is available to provide a legal basis for the activity.

[6] See section 102 of the Act.

Example: An equipment interference agency interferes with a person's device with their consent, which enables a subject's communications and other information to be obtained by surveillance. If the agency considers that the access to the computer material would not be unauthorised and therefore would not constitute a CMA offence, it may obtain an intrusive surveillance authorisation under Part 2 of RIPA to authorise the surveillance. The agency will not require an equipment interference warrant.

2.37 Secondly, the Act does not require a security and intelligence agency to obtain an equipment interference warrant where there is no British Islands connection (even if the conduct to be authorised constitutes an offence under the CMA). Some equipment interference conducted outside of the British Islands will be small-scale and will often take place in difficult and hostile environments which are outside the control of the equipment interference agencies. The window of opportunity within which equipment operations can take place overseas is often small and unpredictable and it will not always be possible or safe to obtain prior individual authorisation for every act undertaken. In these circumstances it will be more appropriate to authorise the necessary conduct under section 7 of the 1994 Act.

2.38 However, the Act does not restrict the ability of an agency to apply for a targeted equipment interference warrant even where it is not mandatory under the Act. In particular this may include circumstances where the activity is taking place outside the British Islands in such a place that the relevant service considers that with regard to the ECHR it may be prudent to obtain a targeted equipment interference warrant. Such activity may include activity within British embassies, military bases and detention centres. Equipment interference agencies should also consider seeking an equipment interference warrant under the Act for targeted operations outside the British Islands if the subject of investigation is a UK national or is likely to become the subject of civil or criminal proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court.

2.39 In any case where communications, private information or equipment data are obtained under sections 5 or 7 of the 1994 Act, a security and intelligence agency must handle the material so obtained in accordance with the safeguards set out in Covert Surveillance and Property Interference Code. Compliance with these safeguards will ensure that the relevant service handles the material in accordance with safeguards equivalent to those set out in chapter 8 of this code[7].

Ministry of Defence

2.40 In common with other equipment interference agencies the Ministry of Defence will obtain an equipment interference warrant for any interference conducted by its civilian or service personnel which might amount to an offence under the CMA and have a connection to the British Islands where the circumstances are such that no defence to such a charge is clearly available (for example, in circumstances where combatant immunity might not apply).

Law enforcement agencies

2.41 Section 14 of the Act restricts the ability of law enforcement agencies to authorise interference with equipment under the 1997 Act. Where the purpose of the interference is to obtain communications, private information or equipment data, activity which was previously authorised under the 1997 Act should now be authorised under Part 5 of the Act, which is subject to enhanced safeguards tailored for this manner of activity.

[7] The Covert Surveillance and Property Interference Code will be updated prior to implementation of the Act.

2.42 As with existing property interference powers in the 1997 Act, this does not prohibit law enforcement agencies from using other powers available to them to access communications, equipment data or other information. In particular, law enforcement officers may continue to exercise their powers of inspection, search or seizure or undertake any other conduct amounting to interference for these purposes that is authorised or required under an enactment or rule of law - for example, where a law enforcement officer interferes with equipment by seizing it pursuant to a warrant issued under the Police and Criminal Evidence Act 1984 as relevant evidence in a criminal investigation. For the avoidance of doubt, and notwithstanding any other provisions of this code, an equipment interference warrant will not be required where the interference is authorised under another law enforcement power.

3 Equipment interference warrants - general rules

Overview

3.1 An equipment interference warrant under Part 5 or Chapter 3 of Part 6 of the Act will provide a lawful basis for an equipment interference agency to carry out equipment interference to obtain communications, equipment data or other information.

3.2 Responsibility for issuing targeted equipment interference warrants, and the purposes for which warrants may be issued, varies depending on the equipment interference agency applying for the warrant. Targeted examination warrants and bulk equipment interference warrants may only be issued by a Secretary of State to a security and intelligence agency. Targeted equipment interference warrants may be issued to the security and intelligence agencies and Defence Intelligence by the Secretary of State. In certain circumstances targeted equipment interference and targeted examination warrants may also be issued to the security and intelligence agencies by the Scottish Ministers. Targeted equipment interference warrants for law enforcement agencies are issued by a relevant law enforcement chief[8].

3.3 Where not otherwise specified this code will refer to the 'issuing authority' to include the Secretary of State, Scottish Minister or law enforcement chief where relevant.

Types of equipment interference warrant

3.4 The Act provides that three types of equipment interference warrant may be issued. Guidance on targeted equipment interference and targeted examination warrants is set out in Chapter 4 of this Code. Guidance on bulk equipment interference warrants is set out in Chapter 5 of this Code.

- A **targeted equipment interference warrant** described in section 94(2) of the Act authorises the person to whom it is addressed to secure interference with any equipment to obtain communications, equipment data or other information. The subject matter to which an equipment interference warrant may relate is specified in section 96.
- A **bulk equipment interference warrant** described in section 163 of the Act is a warrant which meets two conditions. First, it must authorise the person to whom it is addressed to secure interference with any equipment to obtain communications, equipment data or other information. Secondly, its purpose must be to obtain overseas-related communications, overseas-related information or overseas-related equipment data[9]. Material obtained under a bulk equipment interference warrant may only be selected for examination in accordance with the safeguards set out in section 168 of the Act including (where necessary) a targeted examination warrant.

[8] See Annex A for full table of law enforcement issuing authorities.

[9] See Chapter 3 and section 163 of the Act for the meaning of overseas-related communications, overseas-related private information or overseas-related equipment data.

- A **targeted examination warrant** described in section 94(9) of the Act authorises the person to whom it is addressed to carry out the selection for examination of protected material obtained under a bulk equipment interference warrant in breach of the prohibition in section 179(4) of the Act.

Equipment interference agencies

3.5 Only certain public authorities may apply for equipment interference warrants under the Act and only for the relevant specified purposes:

- Applications for targeted equipment interference warrants and targeted examination warrants may be made by or on behalf of the head of a security and intelligence agency on the grounds of national security, preventing or detecting serious crime[10] or the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security;
- Applications for targeted equipment interference warrants may be made by or on behalf of the Chief of Defence Intelligence on grounds of national security;
- Applications for targeted equipment interference warrants may be made by an appropriate law enforcement officer on the grounds of preventing or detecting serious crime or for certain law enforcement agencies, preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health[11].
- Applications for bulk equipment interference warrants may only be made by or on behalf of the head of a security and intelligence agency on grounds of national security, or on the grounds of national security and preventing or detecting serious crime and/or in the interests of the economic well-being of the UK (so far as those are also relevant to the interests of national security). At least one of the grounds for issuing a bulk equipment interference warrant must therefore be national security.

3.6 Warrants must be issued personally by a Secretary of State or the Scottish Ministers in the case of a security and intelligence agency, and by a Secretary of State in the case of Defence Intelligence. Equipment interference warrants for law enforcement agencies must be issued by a law enforcement chief to their relevant law enforcement officer (as listed in section 101 of the Act, see annex A).

3.7 The statutory purposes for which equipment interference warrants may be issued reflect the functions of the agency carrying out the equipment interference. Each of the equipment interference agencies must conduct equipment interference operations in accordance with their statutory or other functions, and the provisions of the Act.

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

[11] Use of equipment interference to prevent death or injury to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health will only be used in exceptional circumstances. In these circumstances equipment interference techniques will most likely be used to assist in locating vulnerable persons. Accordingly, the Act limits the use of equipment interference for this purpose to relevant agencies. The following persons may not apply for warrants for this purpose: Officers of The Competition and Markets Authority, officers of the Police Investigations and Review Commissioner, officers of Revenue and Customs and Immigration Officers. Section 96(2) of the Act restricts this power to the appropriate law enforcement agencies.

3.8 In the case of the Security and Intelligence Agencies:

- For the Security Service, the Security Service Act 1989 provides that the Service's functions are the protection of national security, the safeguarding of the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands and the provision of support to the police and other law enforcement authorities in the prevention and detection of serious crime;
- For the Secret Intelligence Service the 1994 Act provides that its functions are to obtain and provide information relating to the actions or intentions of persons outside the British Islands and to perform other tasks relating to the actions or intentions of such persons in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom, or in the interests of the economic well-being of the United Kingdom or in support of the prevention or detection of serious crime;
- In the case of the GCHQ, the 1994 Act provides, as relevant, that one of its functions is to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom, or in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands, or in support of the prevention or detection of serious crime.

3.9 In the case of Defence Intelligence, as for the Ministry of Defence more generally, its functions derive from the prerogative. The Bill limits the use of equipment interference by the Ministry of Defence to matters concerning national security.

3.10 In the case of the NCA, the Crime and Courts Act 2013 confers functions on the NCA, Director General and NCA officers, which are collectively referred to as 'NCA functions'. The NCA functions are a 'crime reduction function', a 'criminal intelligence function' and a collection of other functions conferred by the 2013 Act and other enactments.

3.11 In the case of other law enforcement bodies, their functions derive from a mixture of statute and common law. For example, a police force is a number of individual constables, whose status derives from the common law, organised together in the interests of efficiency. A member of a police force, of whatever rank, when carrying out his duties as a constable acts as an officer of the Crown and a public servant. The primary duties of those who hold the office of constable are the protection of life and property, the preservation of the Queen's peace and the prevention and detection of criminal offences. In general terms, police forces are therefore responsible for the investigation of crime, collection of evidence and the arrest or detention of suspected offenders.

Incidental conduct

3.12 Where an equipment interference agency obtains an equipment interference warrant, the warrant also authorises any conduct necessary to undertake what is expressly authorised or required by the warrant (excluding conduct that constitutes the interception of live communications[12]).

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

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

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

Example: An equipment interference agency has obtained a warrant to acquire communications and other relevant information from a target's device, which it anticipates gaining covert access to for a brief period of time. During the operation, the agency unexpectedly has access to two devices, and cannot determine whether one or both belong to the target. The agency is permitted to examine both using equipment interference techniques in order to clarify whether one or both belong to the target – this is incidental conduct, which may involve the obtaining of data from both devices. If one device is then found not to be connected to the target, the full equipment interference described in the warrant will not take place against that device and any data already obtained relating to that device will be deleted as soon as possible.

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

Surveillance

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

3.17 A separate authorisation for surveillance under Part 2 of RIPA will not therefore be required providing the conduct comprising the surveillance is properly authorised by a targeted equipment interference warrant. The interference with privacy and property resulting from the equipment interference will be considered as part of the equipment interference authorisation.

3.18 In cases where an equipment interference agency wishes to obtain communications or information by surveillance under a targeted equipment interference warrant, the proposed activity should be set out in the application and be expressly authorised by the warrant.

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

3.20 For example, if an equipment interference agency wishes to conduct separate surveillance on the user of a device at the same time as the device itself is being subject to equipment interference, then this will not be considered as part of the equipment interference authorisation and appropriate surveillance authorisation must be obtained. In this situation a combined warrant may be appropriate (for information on combined warrants, see paragraph 4.80).

Interception

3.21 An equipment interference warrant cannot authorise conduct that would amount to an offence, under section 3(1), of unlawful interception of a communication in the course of its transmission (e.g. live interception of an online video call) except if the warrant authorises the obtaining of a communication stored in or by a telecommunication system. If an equipment interference agency wishes to conduct interception of communications other than stored communications, an interception warrant must be obtained under Part 2 or Chapter 1 of Part 6 of the Act (further guidance on interception warrants may be found in the Interception of Communications Code of Practice).

Example: An equipment interference agency wishes to conduct equipment interference on a device to acquire communications stored on the device and intercept video calls being made from the device, in the course of their transmission. The interception cannot be authorised by an equipment interference warrant, which includes as incidental conduct. An interception and equipment interference warrant must both be obtained (either as a combined warrant or separately).

Necessity and proportionality

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

3.23 If the warrant is considered necessary for any of the purposes specified, the person issuing the warrant must also consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

3.24 In the case of a **bulk equipment interference warrant**, the Act provides that the Secretary of State must consider that the main purpose of the warrant is to obtain overseas-related communications, overseas-related information or overseas-related equipment data. The Secretary of State must also consider the warrant is necessary for one or more statutory purposes, and proportionate to what is sought to be achieved by the conduct.

3.25 The Secretary of State must consider that the selection for examination of any material obtained under the bulk warrant is necessary for one or more specified operational purposes, and that examination for the operational purposes is necessary for the statutory purposes specified in the warrant.

3.26 3.26 **For all equipment interference warrants** the issuing authority must also believe that the equipment interference is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that 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 material which is sought could reasonably be obtained by other less intrusive means.

3.27 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the interference against what is sought to be achieved;
- explaining how and why the methods to be adopted will minimise the risk of intrusion on the subject and others;
- whether the activity is an appropriate use of the legislation.
- whether there are any implications of the conduct authorised by the warrant for the privacy and security of other users of equipment and systems, including the internet, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation;
- evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented; and
- where a bulk equipment interference warrant is available, the safeguards set out in Chapter 3 of Part 6 of the Act.

3.28 In the case of warrants issued under sections 96(1) (g) and (2) (e) of the Act for the purposes of testing and training, proportionality should be considered by assessing the potential for, and seriousness of, intrusion into any affected persons' privacy against the benefits of carrying out the proposed testing or training exercise.

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

Trade Unions

3.30 As set out in clauses 97, 98, 99 and 101 the fact that the information that would be obtained under the a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State, law enforcement chief or Scottish Ministers. Equipment interference agencies are permitted to apply for a warrant against members or officials of a trade union considered to be a legitimate intelligence target where that is necessary for one or more of the statutory purposes and proportionate to what is sought to be achieved.

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

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

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

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

3.33 Any application for an equipment interference warrant should contain an assessment of any risk to the security or integrity of systems or networks that the proposed activity may involve including the steps taken to appropriately minimise such risk according to paragraph 3.31. In particular, any application for an equipment interference warrant that relates to equipment associated with Critical National Infrastructure should contain a specific assessment of any risks to that equipment and the steps taken to appropriately minimise that risk. The issuing authority should consider any such assessment when considering whether the proposed activity is proportionate.

4 Targeted equipment interference warrants

4.1 This section applies to the two kinds of equipment interference warrants that may be issued under part 5 of the Act for the purpose of targeted equipment interference and examination with a warrant. These are:

- Targeted equipment interference warrants; and
- Targeted examination warrants (authorising the selection for examination of protected material obtained under a bulk equipment interference warrant).

4.2 A targeted equipment interference warrant described in section 94(2) of the Act authorises the person to whom it is addressed to secure interference with any equipment to obtain communications, equipment data or other information. A warrant may also authorise the disclosure of material obtained under the warrant.

4.3 Responsibility for the issuing of targeted equipment interference warrants, and the grounds on which the warrant may be issued, depends on the equipment interference agency applying for the warrant. With the exception of urgent warrants (see paragraph 4.50) all decisions to issue equipment interference warrants must be approved by a Judicial Commissioner before they are issued.

4.4 In the case of the **Security and Intelligence Agencies**, warrants must be issued by the Secretary of State on an application made by or on behalf of the head of a security and intelligence agency. The warrant must be necessary in the interests of national security, for the prevention or detection of serious crime or in the interests of the economic well-being so far as those interests are also relevant to the interests of national security[13]. Where the only equipment to be interfered with is in Scotland at the time the warrant is issued, and the warrant is necessary for the purpose of preventing or detecting serious crime, the warrant must be issued by a Scottish Minister.

4.5 In the case of **Defence Intelligence**, warrants must be issued by the Secretary of State on an application made by or on behalf of the Chief of Defence Intelligence. The warrant must be necessary in the interests of national security only.

4.6 In the case of **law enforcement**, warrants may be issued by a law enforcement chief on an application made by a person who is an appropriate law enforcement officer in relation to the chief. The warrant must be necessary for the purpose of preventing or detecting serious crime or for certain law enforcement agencies, preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

4.7 Targeted equipment interference warrants, when issued to the Security and Intelligence Agencies or the Ministry of Defence, are addressed to the person who submitted the application.

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

[13] A warrant will only be considered necessary on these grounds if the interference is necessary to obtain information relating to the acts or intentions of persons outside the British Islands.

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

Format of warrant application

Targeted equipment interference warrants

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

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

b. The subject-matter(s) of the warrant, to include the following information dependent on the subject-matter(s):

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

c. A description of any communications, equipment data or other information that is to be (or may be) obtained;

d. An outline of how obtaining the material will benefit the investigation or operation. The relevance of the material being sought should be explained along with any considerations which might be relevant to the consideration of the application;

e. Sufficient information to describe the type of equipment which will be affected by the interference;

f. A description of the conduct to be authorised as well as any conduct it is necessary to undertake in order to carry out what is expressly authorised or required by the warrant, including whether communications or other information is to be obtained by surveillance;

g. An assessment of the consequences and potential consequences of that conduct, including any risk of compromising the security of any equipment directly or indirectly involved with the interference and, in particular, whether this may enable further intrusion into privacy or impact upon Critical National Infrastructure;

h. In the case of thematic warrants, an assessment of whether it will be reasonably practicable to modify the warrant when the identities of the subjects become known and, if so, when such modifications are expected to occur. Where the warrant applicant believes it will not be reasonably practicable to modify the warrant as the identities of individuals, organisations or relevant locations become apparent they should set out the reasons for this.

i. The nature and extent of the proposed interference;

j. An explanation of why the equipment interference is considered to be necessary on one of the grounds set out in Part 5;

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

l. In the case of law enforcement agencies, the factors considered when determining if it is proportionate for the warrant to be issued to the appropriate law enforcement officer (see paragraph 4.35).

m. What measures will be put in place to ensure proportionality is maintained (for example, the methods by which the material collected will be processed to reduce collateral intrusion (e.g. through filtering or processing the material before any of it is examined), and these can be imposed as conditions on the granting of the warrant.)

n. Consideration of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why that intrusion is justified in the circumstances;

o. Whether the conduct is likely or intended to result in the obtaining of privileged or other confidential material and, if so, what protections it is proposed will be applied to the handling of the information so obtained; Where an application is urgent, the supporting justification;

p. In case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results, and an explanation of the collateral intrusion that has arisen to date and how this has been managed;

q. An assurance that all material obtained will be kept for no longer than necessary and handled in accordance with the safeguards required by section 122 of the Act and chapter 8 of this code.

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

Targeted examination warrants

4.12 **A targeted examination warrant** described in section 94(9) of the Act authorises the person to whom it is addressed to carry out the selection for examination, in breach of the prohibition in section 179(4) of the Act, of protected material obtained under a bulk equipment interference warrant of an individual known for the time being to be in the British Islands.

4.13 Targeted examination warrants must be issued by the Secretary of State on an application made by or on behalf of the head of a security and intelligence agency. An application for a targeted examination warrant should contain the following information:

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

b. The subject-matter(s) of the warrant, to include the following information dependent on the subject-matter(s):

- A warrant that relates to a particular person or organisation must name or describe that person or organisation;
- A warrant that relates to a group of persons who share a common purpose or who carry on, or may carry on a particular activity, must name or describe as many of the persons as it is reasonably practicable to name or describe;
- Where a warrant relates to more than one person or organisation for the purposes of a single investigation or operation, it must describe the nature of the investigation or operation and name or describe as many of the persons or organisations as it is reasonably practicable to name or describe;
- A warrant that relates to testing and training activities must describe the nature of the testing, maintenance or development of capabilities and/or a description of the training;

c. A description of the protected material that is to be selected for examination;

d. An explanation of why the selection for examination is considered to be necessary on one of the grounds set out in Part 5;

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

f. Consideration of any collateral intrusion and why that intrusion is justified in the circumstances;

g. Whether the selection for examination is likely or intended to result in the obtaining of privileged or other confidential material and, if so, what protections it is proposed will be applied to the handling of the information so obtained;

h. Where an application is urgent, the supporting justification;

i. An assurance that any protected material selected will be kept for no longer than necessary and handled in accordance with the safeguards required by section 122 of the Act (see chapter 8).

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

Subject-matter and scope of targeted warrants

4.15 Section 96 sets out the subject-matter of targeted warrants and constrains what equipment can be described in the warrant or what protected material can be selected for examination; this section therefore sets the "scope" of a targeted warrant. Technically, any equipment may be interfered with or protected material selected for examination provided they fall within the warrant's scope. The subject-matter of equipment interference and examination warrants may be targeted or thematic.

Targeted warrants relating to a person, organisation or particular location

4.16 In many cases, equipment interference and examination warrants will relate to **targeted subjects**. Targeted subjects are described in sections 96(1)(a) and (d) and must comprise a particular person, organisation or a particular location. A "person" for these purposes may be an individual but also includes all legal persons, corporate or unincorporate. An "organisation" may additionally include entities that are not legal persons. This means, for example, that a warrant may relate to a particular company; the company is the "person" to which the warrant relates and the warrant will authorise interference with equipment belonging to, used by or in the possession of that company. There is no obligation to name any of the directors and employees etc. of the company in the warrant (see section 108(3)), although the warrant must describe the type of equipment to be interfered with which is likely to include equipment used by those persons. Similarly, in the case of an unincorporated body such as a partnership, a warrant may refer just to the partnership, but will authorise the interference with equipment used by members of that partnership.

4.17 In practice, an application for a targeted warrant of this nature falling within section 96(1)(a) or (d) is likely to be appropriate where the purpose of the warrant is to obtain intelligence about the legal person or organisation itself, rather than the individuals who are directors, employees or members of the company or organisation. The Act does not require the equipment interference agency to name or describe individuals within legal persons or organisations in the warrant; in many cases the identities of these individuals will be irrelevant to the intelligence being sought, their identities will not be known (or could only be ascertained by further interferences with privacy) and it would not provide a meaningful safeguard.

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

Example 1

An organisation set up for procuring items relating to research is suspected of sourcing material for nuclear production in a country subject to UN sanctions. Further information is required about the organisation, the materials it sources, and the shipments of goods going out from the organisation. In this particular case, equipment interference is the least intrusive means of acquiring this information since the intelligence interest is in the organisation and its activities, not the individuals employed by the organisation who may not even be aware of what is going on. EI yields intelligence on the products being shipped to the country in question, confirming these are items that could only be used for nuclear production, and enabling the UN to take action.

Example 2

A military base is situated in a specific location known to be the centre for intercontinental ballistic missile research being undertaken by a country with hostile intentions against the UK. In order to track how the research is evolving and what types of systems are being developed, equipment interference is used to gather intelligence from that specific location. Intelligence reveals that the military base is in a state of readiness to test a recently developed missile and also exposes future plans for using the missile on an attack against the UK should the test be successful. The intelligence allows a UK military unit in the area to take action to safeguard UK national security.

Targeted thematic warrants

4.19 Targeted equipment interference warrants may cover equipment relating to more than one person, organisation or location; these are sometimes referred to as targeted 'thematic' warrants. Targeted thematic warrants can cover a wide range of activity; it is entirely possible for a thematic warrant to cover a wide geographical area or involve the acquisition of a significant volume of data, provided the strict criteria of the Act are met.

4.20 The Act provides for the way in which the subject of targeted warrants must be described; section 108(3) and (5) impose certain additional requirements as to what such warrants must specify. Where a targeted thematic warrant relates to equipment used by a group of persons who share a common purpose, for example, the warrant must name or describe as many of the persons as reasonably practicable. However, the list of persons does not set the scope of the warrant (which is the equipment used by the group) and therefore anyone who falls within the group as described will be within the scope of the warrant. Further guidance on targeted thematic warrants is set out below.

4.21 Section 95(1) of the Act contains the types of subject-matter to which a targeted warrant can relate. Targeted thematic warrants can cover the following subject matters:

a) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity (see section 95(1)(b)). For example, the warrant could authorise the interference with computer equipment associated with a group of individuals who are engaged in or supporting Islamist extremist attack planning in the UK;

b) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation (see section 95(1)(c)). For example, the warrant could authorise interference with the computer equipment of a number of companies that are being used as fronts for serious crime;

c) equipment in more than one location, where the interference is for the purpose of a single investigation or operation (see section 95(1)(e)). For example, the warrant could authorise interference with computer equipment in a number of locations which is believed to be being used in attempts to steal confidential commercial secrets of high financial value from UK technology firms, but where it may not be possible to identify the actor(s) behind the attack;

d) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description (see section 95(1)(f)). For example, the warrant could authorise interference with computers which are all using the same paedophilia file sharing site;

e) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information (see section 95(1)(g)). For example, the warrant could authorise the testing of a new technique to be deployed against computers to help ensure that the technique is effective. A warrant could be applied for where there is a risk of innocent users being impacted, for example if testing utilised a real world service. However, no such warrant would be needed for wholly internal laboratory testing.

f) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment (see section 95(1)(h)). For example, the warrant could authorise training that is being carried out overseas to obtain equipment data from a number of devices owned and operated by the equipment interference agency. In order to obtain the data, these devices are connected to a live data environment which results in real world equipment data being stored on the device. In this example, a warrant is needed to authorise the use of equipment interference for training purposes. However, no such warrant would be required if the devices being targeted are owned and operated by the equipment interference agency and training is undertaken internally using data that has already been obtained under a previous warrant.

4.22 Providing the strict criteria in the Act for necessity and proportionality are met, there is no limit on the number of pieces of equipment relating to persons, organisations or locations which a targeted warrant may cover. The warrant does not need to detail the name or description of the persons, organisations or locations within the scope of a thematic warrant any more than is reasonably practicable at the time of the issue of the warrant. Due to the way in which equipment interference activity is conducted, in that it is targeting equipment rather than individuals, little may be known about the people using the equipment. This may be so, for example, because ubiquitous encryption is in use or the intelligence interest is in information contained on a device irrespective of who is using it. Similarly, the nature of EI techniques and the number of persons potentially covered by the subject-matter of the warrant, such as users of a web forum, would mean that where section 108 requires the warrant to name or describe as many of the persons as it is reasonably practicable to do so, this will often be a description of the class of persons falling within the subject matter, rather than individual names or descriptions. In addition, the nature of the operation or the group being investigated (e.g. a fast-moving operation where there is a threat to life or national security) might mean that it is not reasonably practicable to individually name all members of the group being investigated.

4.23 The thematic warrant application must, though, contain as much information as possible and be as specific as is necessary to enable the issuing authority to foresee the equipment to be covered and assess the scope of the warrant by reference to the group, persons or organisations, locations, activities or testing and training activity. This will ensure that the extent of the reasonably foreseeable interference with privacy caused by the equipment interference, or selection for examination, can be properly and fully assessed by the issuing authority. This enables the issuing authority, and the Judicial Commissioner in his/her review, to be satisfied as to the legality, necessity and proportionality of the conduct authorised. This will also assist those executing the warrant so that they are clear as to the scope of the warrant.

4.24 Where an equipment interference agency becomes aware of equipment belonging to, used by or in the possession of a new person, organisation or location within the authorised scope of a targeted thematic warrant and wishes to start interfering with that equipment, section 108 of the Act contains an ongoing duty to name or describe as many of the persons, organisations or locations which fall within the matter to which the warrant relates, as it is reasonably practicable to do so[14]. If it is reasonably practicable to do so, the new person, organisation or location must be added to the warrant through a modification, but a modification in these circumstances does not alter the scope of the warrant.

4.25 Section 108 only requires an equipment interference agency to seek a modification to add a name or description when it is reasonably practicable to do so. It may not be reasonably practicable, for example, in a fast moving threat to life operation or in a malware case where the agency is more interested in the pattern of behaviour of the actors, their methods and equipment rather than identifying persons involved. In no circumstances is it permitted to modify a warrant so as to authorise conduct falling outside the scope of the original warrant.

4.26 Whether or not it is reasonably practicable to modify a warrant to name or describe additional persons, organisations or locations will depend upon the operation to which the warrant relates. It is likely to be reasonably practicable to make such modifications in cases where there is not a requirement to act quickly due to a limited opportunity to carry out what is authorised by the warrant, or where the quantity and frequency of such modifications would not have a disproportionately adverse impact on the operations of the equipment interference agency.

4.27 For example, an equipment interference agency may have sought a thematic warrant relating to members of an organised crime group involved in the production of counterfeit travel documents. The warrant authorises interference with the equipment used by the group of persons carrying out the counterfeiting activity and names a number of individuals known to be involved, but also authorises interference with the equipment of as yet unidentified individuals that may be assisting the known criminals. If the agency discovers the identity of a new individual involved in the operation and wishes to interfere with equipment being used by that person, the warrant may be modified to include that individual's name or description. As the operation is not time critical and only one additional member has been identified it would be reasonably practicable to add the description of the newly identified individual to the warrant. This will assist the issuing authority in understanding which communications, equipment or other information are being obtained or selected, and will assist a judicial commissioner's oversight of the warrant.

[14] The duty to name or describe as many persons, organisations or locations as it is reasonably practicable to do so applies to warrants that have the subject matter of equipment belonging to, used by or in the possession of persons who form a group which shares a common purpose or who carry on, or may carry on, a particular activity; equipment used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation; and equipment in more than one location, where the interference is for the purpose of a single instigation or operation.

4.28 However, it may not be reasonably practicable to make such modifications, for example:

Example 1: An equipment interference agency is investigating a kidnapping and a warrant has been issued authorising the interference with equipment being used by members of the criminal group associated with the kidnapping. In this situation the time required to modify the warrant as new members of the criminal group are identified would adversely affect the agency's ability to carry out the authorised interference. The original warrant already authorises the required interference into the criminal group and the operation may therefore continue. If the warrant remains necessary for a longer period of time, it may become reasonably practicable to modify the warrant to include the identities listed in the warrant at a later date or upon renewal.

Example 2: An equipment interference agency is conducting an investigation into the pattern of behaviour of persons using a website to disseminate images of child sexual exploitation and a warrant has been issued authorising interference with equipment being used by more than one person to disseminate images via the website. In such a case naming or describing the persons involved in a meaningful way may not be possible due to the number of users of the website or without further unnecessary intrusion in to privacy. Furthermore, the frequency with which online identities change would make repeated modifications unreasonably constraining. The original warrant authorises interference with the equipment of the persons suspected of using the website for criminal purposes.

4.29 When issuing a thematic warrant it is important for the issuing authority to understand whether it is likely to be reasonably practicable to make modifications on the identities of individuals, organisations or relevant locations if they become apparent during the course of an operation.

4.30 The warrant application should therefore contain an assessment of whether it will be reasonably practicable to provide such modifications and, if so, when such modifications are expected to occur. Where the warrant applicant believes it will not be reasonably practicable to modify the warrant as the identities of individuals, organisations or relevant locations become apparent they should set out the reasons for this. This information will assist the issuing authority and Judicial Commissioner when considering if a warrant is necessary and proportionate.

4.31 Where it is not reasonably practicable for a thematic warrant to be modified when the identities of individuals, organisations or relevant locations become apparent over the course of an operation the warrant applicant must still provide the most up to date details in relation to the matters outlined in paragraph 4.10 upon renewal of the warrant. This will ensure that the issuing authority and Judicial Commissioner are able to fully assess whether the activity authorised by the warrant remains necessary and proportionate

4.32 If the issuing authority is able to foresee the extent of all of the interferences to a sufficient degree, including the degree of collateral material present at the time when examination of the material takes place, can therefore properly and fully assess necessity and proportionality and agrees that it is necessary and proportionate, then a thematic warrant can be granted. In such cases, the additional access controls which form an integral part of the bulk warrant regime are not required, given the issuing authority can adequately assess and address all of the relevant considerations at the time of issuing the warrant. By contrast, if it is not possible to so assess the necessity and proportionality of all of the interferences at the time of issuing the warrant, or the assessment is that in the circumstances it would not be proportionate to issue a thematic warrant, then a bulk warrant with its second stage authorisation process might be more appropriate if available.

4.33 In some instances it may not be possible to identify individual pieces of equipment or be specific about the nature of the equipment to be interfered with in advance, or there may be a technique that in itself carries out a specific small amount of interference, but enables access to the data that may already have been granted under an existing authorisation. In these cases the warrant should be specific about the technique and the circumstances in which the warrant is to be used. In such cases, the circumstances must be described in a way that enables the requirements of section 101 of the Act to be met.

4.34 There is an on-going duty to review the necessity and proportionality of warrants and to cancel them as necessary. This duty is especially important for thematic warrants given their scope is potentially wider.

Example 1: Intelligence has suggested that a number of unidentified criminal associates are planning to imminently commit a serious criminal offence. An equipment interference agency may wish to deploy equipment interference against the members of the group planning the offence. As the intelligence picture develops, the equipment interference agency expects to rapidly identify the potential offenders and the exact equipment that they are using. The agency obtains an equipment interference warrant relating to the equipment belonging to, or used by, a group of persons who are carrying on a particular activity (i.e. the planned offence) so they do not have to wait to get a new authorisation each time they identify a new member of the group and a new piece of equipment. However, the duty at section 107 would apply so that the warrant would need to be modified to add the name or description of as many of the persons if it was reasonably practicable to do so.

Example 2: Intelligence suggests that a Daesh-inspired cell dispersed across a small number of locations in the Middle East is plotting an imminent bomb attack against UK interests in the region. Interception reveals that the cell members are all using a unique technique to hide their identities online, known as an anonymisation package. After using equipment interference to obtain equipment data from a large number of devices in the specific locations, a search term ('selector') that is unique to the anonymisation package is applied to the data collected, ensuring that only data relating to the cell members is available for analysis. Using information from the initial analysis, the content from the cell members' devices is then obtained. As the cell members can be identified from their association to a specific, known anonymisation package, a targeted 'thematic' warrant is suitable.

Authorisation of a targeted equipment interference warrant

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

- The warrant is necessary in the case of Security and Intelligence Agencies:[15]
  - In the interests of national security;
  - For the purpose of preventing or detecting serious crime;
  - In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security. A warrant will only be considered necessary on this ground if the information relates to the acts or intentions of persons outside the British Islands.
- The warrant is necessary in the case of law enforcement agencies:
  - For the purpose of preventing or detecting serious crime;

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

- in the case of law enforcement agencies listed in Part 1 of Schedule 6 of the Act
- for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

- The warrant is necessary in the case of Defence Intelligence:
  - In the interests of national security.
- **The conduct authorised by the warrant is proportionate to what it seeks to achieve.** In considering necessity and proportionality, the issuing authority must take into account whether the information sought could reasonably be obtained by other means.
- **There are satisfactory safeguards in place.** The issuing authority must consider that satisfactory arrangements are made for the purposes of the safeguards in section 122 of the Act. These safeguards relate to the copying, dissemination, retention of material obtained by equipment interference and are explained in Chapter 8 of this code.
- **The Secretary of State has consulted the Prime Minister** where the additional protection for Members of Parliament and other relevant legislatures applies (see section 106 of the Act).
- **Judicial commissioner approval.** Except in an urgent case, the issuing authority may not issue a warrant unless and until the decision to issue the warrant has been approved by a Judicial Commissioner. Section 103 of the Act sets out that the Judicial Commissioner must review the conclusions that have been reached as to whether the warrant is necessary on one or more of the grounds and whether the conduct that would be authorised is proportionate to what is sought to be achieved.

Authorisation of a targeted equipment interference warrant: senior officials and appropriate delegates

4.36 When it is not reasonably practicable for the Secretary of State or law enforcement chief to sign an equipment interference warrant a delegate may sign the warrant on their behalf. Typically this scenario will arise where the appropriate Secretary of State or law enforcement chief is not physically available to sign the warrant because, for example, they are on a visit or, in the case of a Secretary of State, in their constituency. Where the warrant is required by a Security and Intelligence Agency, or Defence Intelligence, the Secretary of State or member of the Scottish Government must still personally authorise the equipment interference. When seeking authorisation the senior official must explain the case, either in writing or orally, to the Secretary of State and this explanation should include considerations of necessity and proportionality. Once authorisation has been granted the warrant may be signed by a senior official. If the Secretary of State refuses to authorise the warrant the warrant must not be issued. When a law enforcement chief is unable to sign and issue a warrant an appropriate delegate[16] may exercise the power to issue the warrant. When a warrant is issued in this way the warrant instrument must contain a statement to that effect. Except in urgent cases, the decision to issue the warrant must then be approved by a Judicial Commissioner before the warrant is issued.

[16] Appropriate delegates are listed in Annex A.

Authorisation of equipment interference techniques for law enforcement agencies

4.37 Law enforcement chiefs may only issue an equipment interference warrant if they consider that it is proportionate for the warrant to be issued to their appropriate law enforcement officer. In addition to the factors set out in paragraph 4.35 above, in considering whether it is proportionate, the law enforcement chief should consider the full context of the application, including:

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

4.38 The Secretary of State may issue further guidance to assist law enforcement chiefs in considering whether it is proportionate to issue a warrant to their appropriate law enforcement officer. These considerations will ensure that equipment interference techniques are deployed by law enforcement agencies in a consistent and proportionate manner.

4.39 Some law enforcement agencies may only carry out equipment interference for the purpose of preventing or detecting serious crime when also in relation to specific functions of their agency. These are:

- For immigration officers, the serious crime must relate to an offence which is an immigration or nationality offence;
- For Revenue and Customs, the serious crime must relate to an assigned matter within the meaning of section 1(1) of the Customs and Excise Management Act 1979;
- For a designated customs official, the serious crime must relate to a matter in respect of which a designated customs official has functions; and,
- For the Competition and Markets Authority, the serious crime must relate to offences under section 188 of the Enterprise Act 2002.

Collateral intrusion

4.40 Before authorising applications for equipment interference warrants, the person issuing the warrant should also take into account the risk of obtaining communications, equipment data or other information about persons who are not the targets of the equipment interference activity (collateral intrusion). Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament[17] and another person on constituency business may be involved.

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

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

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

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

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

[17] 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.

Power of Scottish Ministers to issue warrants

4.44 Equipment interference warrants may be issued on "serious crime" grounds by Scottish ministers, by virtue of arrangements under the Scotland Act 1998. The functions of the Scottish ministers also cover renewal, modification and cancellation arrangements. Sections 98 of the Act makes provision for Scottish Ministers to issue targeted equipment interference warrants for serious crime purposes in certain circumstances. Scottish Ministers may issue a targeted examination warrant for serious crime purposes providing the warrant, if issued, would relate only to a person that would be in Scotland at the time of the issue of the warrant or whom the Secretary of State believes would be in Scotland at that time.

Judicial commissioner approval

4.45 Before a targeted equipment interference warrant comes into force, its issuance must be approved by a Judicial Commissioner. Section 103 of the Act sets out the test that a Judicial Commissioner must apply when deciding whether to approve the issuance of an equipment interference warrant. This includes reviewing the warrant issuer's conclusion on whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved.

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

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

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

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

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

Urgent authorisation of a targeted equipment interference warrant

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

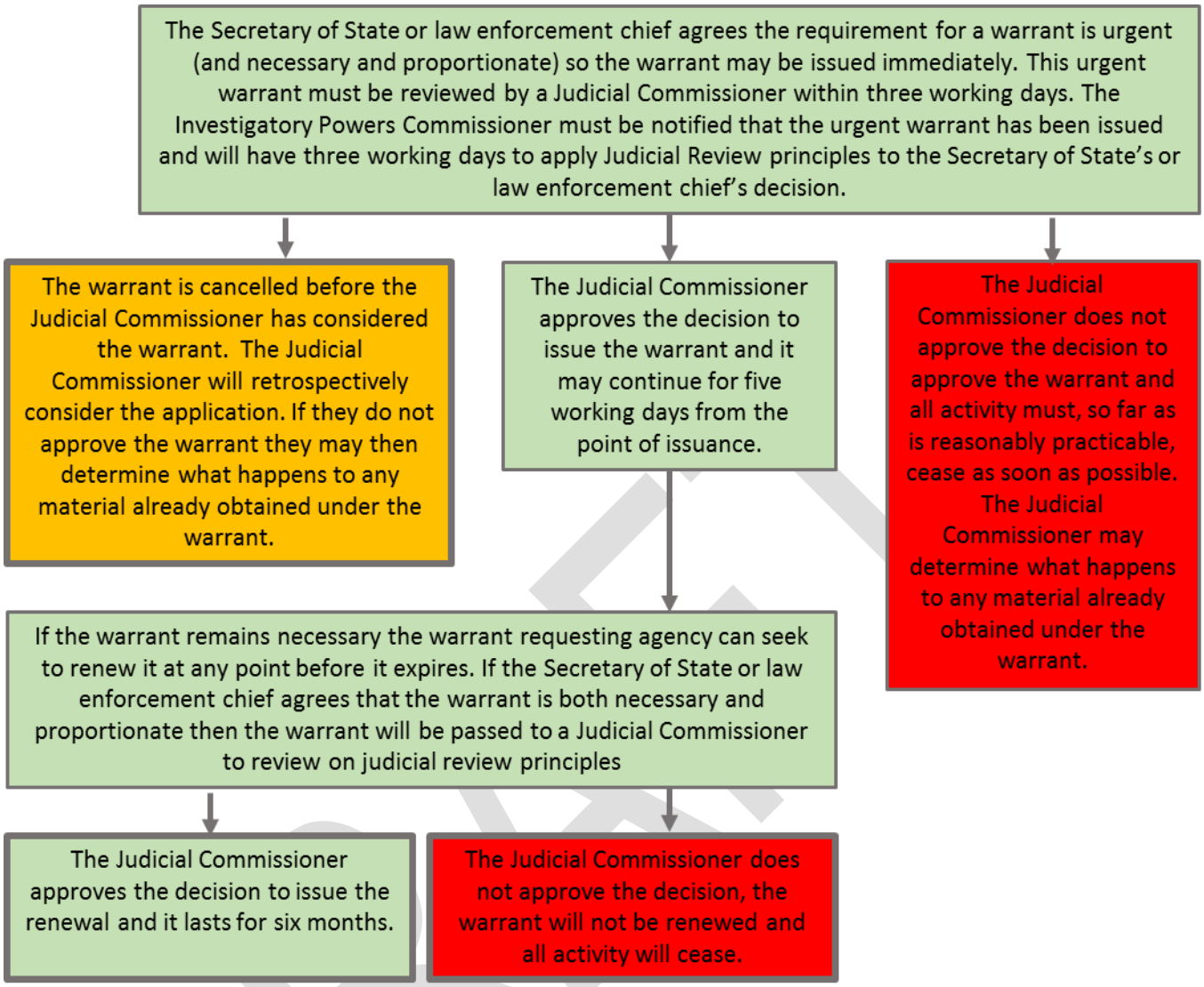
4.51 What constitutes an urgent case is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the requisite time. The requisite time reflects when the authorisation needs to be in place to meet an operational or investigative need.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

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

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

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

4.54 The following diagram illustrates the urgent authorisation process:



Warrants ceasing to have effect and retrieval of equipment

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

4.56 The equipment interference agency may make representations to the Judicial Commissioner about the following matters:

- Whether further equipment interference should be authorised to enable the agency to secure that anything in the process of being done under the warrant stops as soon as possible;
- destruction of any material obtained under the warrant; and
- the conditions that should be imposed as to the use or retention of any of that material.

Format of equipment interference warrants

4.57 The warrant must describe the type of equipment that is to be interfered with and the conduct that the person to whom the warrant is addressed is authorised to take. The warrant must include the details specified in the second column of the Table in section 108 of the Act that relate to relevant equipment described in the first column.

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

- A statement that it is a targeted equipment interference warrant;
- The subject of the equipment interference to which the warrant relates[18]. Where required, descriptions on the instrument can be in the form of an alias or other description that identifies the subject;
- A warrant reference number; and
- The persons who may subsequently modify the warrant in an urgent case (if authorised in accordance with section 112 of the Act).

4.59 An equipment interference warrant may expressly authorise the disclosure of any material obtained under the warrant. However, a warrant does not need to specify all potential disclosures of material. Disclosure of material is permitted provided that it is not an unauthorised disclosure for the purposes of section 124 of the Act. This may include, for example, disclosure of material for admission as evidence in criminal and civil proceedings.

Duration of equipment interference warrants

4.60 Targeted equipment interference warrants and targeted examination warrants issued using the standard procedure are valid for an initial period of six months. Warrants issued under the urgency procedure are valid for five working days following the date of issue unless renewed by the issuing authority.

4.61 Upon renewal, warrants are valid for a further period of six months. This period begins on the day after the day on which the warrant would have expired, had it not been renewed. In practice this means that if a warrant is due to end on 3 March but is renewed on 1 March, the renewal takes effect from 4 March and the renewed warrant will expire on 3 September. An equipment interference warrant may only be renewed in the last 30 days of the period for which it has effect.

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

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

4.64 Where a change in circumstance leads the equipment interference 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 issuing authority that it should be cancelled with immediate effect.

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

Modification of a targeted equipment interference warrant

4.65 Equipment interference warrants may be modified under the provisions of sections 111 and 116 of the Act. The modifications that may be made are:

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

4.66 The modifications above may be made providing that the conduct authorised by the modification is within the scope of the original warrant. It is for this reason that section 111(3) prohibits modifications to add, vary or remove the name or descriptions of a targeted warrant that relates to just one specified person, organisation or location, as such a modification would go beyond the original scope of the targeted warrant. In practice this means that a warrant which relates to a targeted subject cannot be modified into a targeted thematic warrant; a fresh warrant would be required. Modifications to add names or descriptions, which fall within the scope of the original warrant, are required to be made to targeted thematic warrants when it is reasonably practicable to do so (see para 4.25).

4.67 Three examples are provided below – the first would not be permitted, but the second and third would be:

Example of a modification that would not be permitted:
An equipment interference agency obtains a targeted equipment interference warrant relating to equipment associated with a specific serious criminal known as 'Mr. Big'. The issuing authority, with Judicial Commissioner approval, issues the warrant authorising the interference of equipment of 'Mr. Big'. The investigation progresses and the equipment interference agency wants to interfere with the equipment of one of 'Mr. Big's' associates. This would require a new warrant – the warrant against 'Mr. Big' cannot be modified so it is against an additional person.

Example of a modification that would be permitted:
An equipment interference agency obtains a targeted thematic equipment interference warrant relating to equipment associated with a specific serious criminal known as 'Mr. Big' and his unidentified associates. The issuing authority, with Judicial Commissioner approval, issues the warrant authorising the interference of equipment of "'Mr. Big' and his unidentified associates investigated under Operation NAME". The investigation progresses and the equipment interference agency wants to interfere with the equipment of one of 'Mr. Big's' associates. The warrant could be modified to add the name or description of the associate, if reasonably practicable to do so, and the associate's equipment if it did not fall within the type of equipment already described on the warrant.

Example of a modification to add a new subject matter but still stay within the scope of the original warrant: An equipment interference agency obtains a targeted thematic equipment interference warrant relating to equipment associated with a specific malware attack against UK critical national infrastructure. Initially the subject matter of the warrant is defined as clause 96(1)(e) – equipment in more than one location, where the interference is for the purpose of a single investigation or operation. Data obtained indicates that the same equipment is being used for stealing high financial value commercial secrets from a financial institution. In order to investigate the secondary activity, the warrant could be modified to include a new subject matter clause 96(1)(b) – equipment belonging to, used by, or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity. The same devices are targeted and the same conduct is used to obtain the data for both the malware attack and the theft, so the scope of the warrant stays the same.

4.68 A modification may be made by the following persons in circumstances where the person considers that the modification is necessary on any relevant grounds:

- The Secretary of State, in the case of a warrant issued by the Secretary of State;
- A member of the Scottish Government, in the case of a warrant issued by the Scottish Ministers
- A senior official acting on behalf of the Secretary of State or (as the case may be) the Scottish Ministers, or
- A law enforcement chief or the chief's appropriate delegate, in the case of a warrant issued by a law enforcement chief or the chief's appropriate delegate.

4.69 As soon as is reasonably practicable after a person makes a modification to a warrant, a Judicial Commissioner must be notified of the modification and the reason for making it. This does not apply if:

- the modification is an urgent modification (where different notification provisions are provided for, detailed below at Paragraph 4.71),
- sections 106 or 107 apply, or
- the modification is to remove any matter, name or descriptions included in the warrant in accordance with section 108 (3) to (5).

4.70 In the case of a modification of a warrant issued to a law enforcement officer, the decision to make a modification must be approved by a Judicial Commissioner. This ensures that independent consideration is applied to applications for modifications. In the case of a modification of a warrant issued to a security and intelligence agency or Ministry of Defence, the decision to approve a modification can be made by a senior official in the warrant granting department. Where a modification of a warrant is made by a senior official, the Secretary of State or (in the case of a warrant issued by the Scottish Minister) a member of the Scottish Government must be notified personally of the modification and the reasons for making it.

Administrative clarifications of targeted warrants

4.71 Sections 111(5) and 116(11) clarify that a modification is only required where the conduct authorised by the warrant is affected. For example, where more detail is provided for clarification, such as the full name of a person as it becomes known rather than an alias, the administrative clarification will be covered by sections 111(5) and 116(11) as long as the subject of the equipment interference is still accurately described (i.e. there is not a change in the scope of the equipment interference). Similarly, an equipment interference agency may wish to update the subject matter of a thematic warrant from time to time without modifying the scope of the conduct authorised, or the equipment to be interfered with, in which case the modification will fall within this provision. Nonetheless, equipment interference agencies should take measures to keep warrant granting departments up to date with any new information.

Example: An equipment interference agency obtains a warrant against equipment used by a criminal front company to facilitate serious crime. This company regularly changes the name it trades under but the criminal activity behind it and the equipment used remains constant. There is no change in the scope of the warrant but the granting department is kept up to date periodically with the list of names used by the company.

Urgent modification of targeted warrants

4.72 Sections 115 and 117 of the Act make provision for cases in which modifications of a targeted warrant are required urgently. A modification will only be considered urgent if there is a very limited window of opportunity to act. For example, this may include a threat to life situation, where a kidnap has taken place, in the immediate aftermath of a major terrorist incident or where intelligence has been received that a significant quantity of drugs is about to enter the country. In some cases, the modification will necessarily be short-lived, for instance if a kidnap is quickly resolve.

4.73 For the Security and Intelligence Agencies, a senior official in the equipment interference agency may make the urgent modification but it must be approved by a senior official in the warrant granting department within five working days. A judicial commissioner must be notified as soon as is reasonably practicable after the senior official in the warrant granting department makes a decision and the Secretary of State or member of Scottish Government will also be notified personally. In the event that the warrant granting department does not agree to the urgent modification, the activity conducted under the urgent modification up to that point remains lawful. The senior official in the warrant granting department may authorise further interference, but only in the interest of ensuring that anything being done is stopped as soon as possible. The Secretary of State should be informed of any additional interference that has been authorised.

4.74 In the case of law enforcement agencies, the relevant law enforcement chief or an appropriate delegate may make the urgent modification. The modification then must be considered by a judicial commissioner within five working days. In the event that the judicial commissioner does not agree to the urgent modification, the activity conducted under the urgent modification remains lawful. If the judicial commissioner refuses to approve the decision to make a modification they may authorise further interference, but only in the interest of ensuring that anything being done by virtue of the modification is stopped as soon as possible.

Renewal of a targeted equipment interference warrant

4.75 Section 110 of the Act sets out that the appropriate person may renew a warrant at any point before its expiry date. Applications for renewals of warrants should contain an update of the matters outlined in paragraph 4.10 above. In particular, the applicant should give an assessment of the value of equipment interference to date and explain why it is considered that equipment interference continues to be necessary for one or more of the relevant grounds, and why it is considered that the interference continues to be proportionate. Consideration of the extent (if any) of collateral intrusion that has occurred to date, and how this has been managed, will be relevant to the consideration of proportionality. Sections 106 (additional protection for Members of Parliament) and 107 (items subject to legal professional privilege) apply in relation to the renewal of warrants in the same way as they apply to a decision to issue a warrant.

4.76 In all cases, a warrant may only be renewed if the renewal has been approved by a Judicial Commissioner. An equipment interference warrant may only be renewed in the last 30 days of the period for which it has effect.

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

Warrant cancellation

4.78 Any of the persons authorised to issue warrants under Part 5 may cancel a warrant at any time. If an appropriate person[19] within the issuing authority considers that such a warrant is no longer necessary or that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct, the appropriate person must cancel the warrant. Equipment interference agencies therefore will need to keep their warrants under review and must notify the issuing authority if the equipment interference agency assess that the warrant is no longer necessary or proportionate. In practice, in the case of the Security and Intelligence Agencies and Defence Intelligence, the responsibility to cancel a warrant will be normally exercised by a senior official in the warrant granting department on behalf of the Secretary of State. The equipment interference agency should take steps to cease the interference as quickly as possible if they consider that the warrant is no longer necessary or proportionate – they should not wait until the necessary cancellation instrument has been signed.

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

[19] Section 118 (4) define ‘appropriate persons’

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

Combined warrants

4.81 Where an equipment interference agency wishes to conduct equipment interference but not all of the proposed conduct can properly be authorised under an equipment interference warrant, additional warrants or authorisations will be required. The agency may either obtain a combined warrant or may obtain separate warrants/authorisations pursuant to the Act and RIPA, the 1997 Act and/or the 1994 Act.

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

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

4.83 For combinations of warrants under schedule 8, the authorisation process set out at paragraph 4.35 onwards will apply. In some cases this will necessitate a higher authorisation process than would otherwise be required for individual warrant applications. Where two warrants are combined that would otherwise be issued by different authorities (for example, an equipment interference warrant issued by a law enforcement chief and an interception warrant issued by a Secretary of State), the warrant will always be issued by the higher authority level. Where part of a combined warrant is cancelled, the whole warrant ceases to have effect under the same procedures set out at paragraph 4.78.

4.84 Where warrants are sought urgently and the intention is to later proceed with a combined warrant application, such an application must be made before the urgent warrant authorisation ceases to have effect.

4.85 Per paragraph 20(1)(a) of Schedule 8, the duties imposed by clause 2 (having regard to privacy) apply to combined warrants as appropriate, e.g. when issuing, renewing or cancelling a Part 2, 5, 6 or 7 warrant, modifications, granting/approving or giving/varying/revoking notices. So the targeted equipment interference element of a combined warrant cannot be issued without having regard to privacy per clause 2.

4.86 The exclusion of matters from legal proceedings (section 53) continues to apply to an interception warrant that is part of a combined warrant. However, when an equipment interference warrant is combined with an interception warrant the material derived from equipment interference may still be used in legal proceedings if required. If material derived from equipment interference authorised by a combined warrant can be recognised as a product of interception, and therefore reveals the existence of a warrant issued under Chapter 1 of Part 1 of the Act, the material is excluded from use in legal proceedings according to section 53 of the Act.

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

Applications made by or on behalf of the Security and Intelligence Agencies

4.88 Paragraph 1 of Schedule 8 sets out that the Secretary of State may issue a warrant that combines a targeted interception warrant with a targeted equipment interference warrant issued under section 19. Such warrants will only be available to agencies that can apply for equipment interference warrants and interception warrants. Paragraph 8 of Schedule 8 sets out that the Secretary of State may also combine a targeted equipment interference warrant under section 97 with one or more of the following:

- A targeted examination warrant under section 1(2) or section 97(3)
- A directed surveillance authorisation under section 2 of RIPA
- An intrusive surveillance authorisation under section 2 of RIPA
- A property interference authorisation under section 5 of the Intelligence Services 1994

4.89 Paragraph 4 sets out that a Scottish Minister may issue a warrant combining a targeted equipment interference warrant under section 98(1) with a targeted interception warrant under and/or a targeted examination warrant under section 21.

4.90 Paragraph 8 of Schedule 8 sets out that the Secretary of State may issue a warrant that combines a targeted equipment interference warrant with one or more of the following:

- A targeted examination warrant under section 97(3)
- A directed surveillance authorisation under section 2 of RIPA
- An intrusive surveillance authorisation under section 2 of RIPA
- A property interference authorisation under section 5 of the Intelligence Services Act 1994

Example: A security and intelligence agency wishes to conduct an operation which involves intrusive surveillance (provided for under section 5 of the Intelligence Services Act) and targeted equipment interference. Under Schedule 8 they may wish to combine these applications, so that the combined warrant is issued by the Secretary of State. In approving the decision to issue the warrant, the Judicial Commissioner would only consider the application for targeted equipment interference. Intrusive surveillance under section 5 of the 1994 Act cannot be combined with warrants outside of the Act e.g. Directed Surveillance Authorisations under Part 2 of RIPA.

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

4.91 Paragraph 9 of Schedule 8 sets out that the Secretary of State may, on an application made by or on behalf of the Chief of Defence Intelligence, issue a warrant that combines a targeted interception warrant with a targeted equipment interference warrant.

Applications made by or on behalf of a relevant law enforcement agency

4.92 Paragraph 11 of Schedule 8 sets out that the law enforcement chief may issue a warrant that combines a targeted equipment interference warrant with one or more of the following:

- A directed surveillance authorisation under section 2 of RIPA
- An intrusive surveillance authorisation under section 2 of RIPA
- A property interference authorisation under the 1997 Act

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

Example 2: An equipment interference agency wishes to conduct an operation which involves directed surveillance (provided for under Part 2 of RIPA) and targeted equipment interference. Under Schedule 8 they may wish to combine these applications. For a warrant issued to the head of an intelligence service the combined warrant would be issued by the Secretary of State and approved by a Judicial Commissioner. For a law enforcement agency, the relevant law enforcement chief would consider the directed surveillance activity as part of the entire combined applications. This entire combined application would also require approval by a Judicial Commissioner.

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

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

Collaborative working

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

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

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

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

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

- Applications for equipment interference warrants by police forces must only be made by a member or officer of the same force as the law enforcement chief, unless the chief officers of the forces in question have made a collaboration agreement under the Police Act 1996 and the collaboration agreement permits applicants and law enforcement chiefs to be from different forces.
- Applications for equipment interference warrants by law enforcement agencies other than police forces must only be made by a member or officer of the same force or agency as the law enforcement chief regardless of which force or agency is to conduct the activity.

4.99 Without limiting the ability of equipment interference agencies to work collaboratively, as out lined above, applications for equipment interference warrants may only be issued to a member of the same equipment interference agency as made the application, except where specified law enforcement agencies have entered into a relevant collaboration agreement under the Police Act 1996 which permits this rule to be varied.

4.100 This exception only applies to police forces and the National Crime Agency, where they are able to enter into collaboration agreements under the Police Act 1996. The collaboration agreement must permit the law enforcement chief of one collaborating law enforcement agency to issue a warrant to an applicant from another collaborating law enforcement agency.

4.101 Where, pursuant to a collaboration agreement, the Director General of the National Crime Agency is the law enforcement chief for an application made by a member of a collaborative police force, the Director General may only issue the warrant if he considers there is a British Islands connection. This reflects the general restriction that warrants should only be issued to police forces where there is a British Islands Connection (see further at paragraph 2.33).

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

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

4.104 Where an equipment interference agency requires an international partner– who is not therefore an equipment interference agency as defined by the Act – to undertake an action authorised by an equipment interference warrant, this must be clearly specified within the warrant application. The application must make clear why the assistance of an international partner is required and specify the activity that the equipment interference agency intends to request of that partner. Once a warrant is issued, an equipment interference agency may work collaboratively with an international partner to carry out equipment interference in accordance with that warrant by virtue of section 94 (5) (b) of the Act.

5 Bulk equipment interference warrants

5.1 This Chapter provides guidance on bulk equipment interference warrants issued under Chapter 3 of Part 6 of the Act and the safeguards that apply to the selection for examination of material obtained under such a warrant. Bulk equipment interference warrants and targeted examination warrants may only be issued to the Security and Intelligence Agencies.

5.2 The safeguards that apply to the access, retention, disclosure, deletion and destruction of all communications, information and equipment data obtained under targeted and bulk equipment interference warrants are set out in Chapter 8 of the code.

Bulk equipment interference

5.3 Bulk equipment interference warrants are described in section 163 of the Act. Under bulk warrants, the subsequent examination of any material collected under the warrant is controlled by additional statutory access controls (e.g. operational purposes, necessity and proportionality tests). Further safeguards are applied to the examination of communications and private information of individuals within the British Islands – a separate targeted examination warrant, subject to the full "double-lock" authorisation process, is required to examine this material.

5.4 Bulk warrants will usually only be appropriate for large scale operations, and are only available for operations for the obtaining of overseas related communications, overseas-related information or overseas-related equipment data.

5.5 To determine whether a thematic or bulk warrant is appropriate, regard must be given in particular to whether the Secretary of State is able to foresee the extent of all of the interferences to a sufficient degree to properly and fully assess necessity and proportionality *at the time of issuing the warrant*. This includes consideration of interferences in relation to all those individuals affected, whether the intended target of the interference or those affected incidentally. Where this can be done, usually due to the specific identity of the target being known in advance or a specific identifier relating to the target individuals' communications or devices, a thematic warrant is likely to be most appropriate. This is because the additional access controls of the bulk regime are not required if a greater degree of targeting, or the filtering or processing of data at or soon after the point of collection, can limit interference such that the Secretary of State and the Judicial Commissioner can adequately address all of those considerations (e.g. necessity and proportionality, purpose, protection for UK persons' content) from the outset. Based on the scenario given at 4.34, the following example demonstrates the difference between thematic and bulk equipment interference:

Example: Intelligence suggests that a Daesh-inspired cell in a particular location in the Middle East is plotting an imminent bomb attack against UK interests in the region. Little is known about the individual members of the terrorist cell. However, it is known that a particular software package is commonly – but not exclusively – used by some terrorist groups. After using equipment interference to obtain equipment data from a large number of devices in the specified location, analysts apply analytical techniques to the data, starting with a search term ('selector') related to the known software package, to find common factors that indicate a terrorist connection. A series of refined searches of this kind, using evolving factors that are uncovered during the course of the analytical process, gradually identify devices within the original 'pot' of data collected that belong to the terrorist cell. Their communications (including content) can then be retrieved and examined.

As the cell members can only be identified through a series of refined searches that cannot all be assessed in advance at the time the warrant is issued, second stage access controls are required to govern all of the data selection within the operation. Accordingly, a bulk equipment interference warrant is suitable.

Application for a bulk equipment interference warrant

5.6 An application for a bulk equipment interference warrant is made to the Secretary of State. As set out at section 165 of the Act, bulk equipment interference warrants are only available to the Security and Intelligence Agencies. An application for a bulk equipment interference warrant therefore may only be made by or on behalf of the following persons:

- The Director General of the Security Service;
- The Chief of SIS;
- The Director of GCHQ.

5.7 Bulk equipment interference warrants, when issued, are addressed to the head of the security and intelligence agency by whom, or on whose behalf, the application was made. A copy may then be served on any person who may be able to provide assistance in giving effect to that warrant. The purpose of such a warrant will typically reflect one or more of the intelligence priorities set by the National Security Council (NSC)[20].

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

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

- Background to the operation in question:
  - A general description of the equipment to be interfered with and the communications, information and equipment data to be obtained; and
  - Description of the conduct to be authorised, which must be restricted to the obtaining of overseas-related communications, overseas-related information or overseas-related equipment data, or the conduct (including the obtaining of other communications, information or equipment data not specifically identified by the warrant as set out at section 163(5)) that is necessary to undertake in order to carry out what is authorised or required by the warrant.

[20] One of the NSC's functions is to set the priorities for intelligence coverage for GCHQ and SIS.

- An assessment of the consequences (if any) and potential consequences of the conduct, including any risk of compromising the security of any equipment directly or indirectly involved with the interference and, in particular, whether this may enable further intrusion into privacy;
- The operational purposes for which the material obtained may be selected for examination and an explanation of why examination is necessary for those operational purposes proposed in the warrant;
- An explanation of why the equipment interference is considered to be necessary for one or more of the statutory purposes, which must always include an explanation of why the equipment interference is necessary in the interests of national security;
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, explaining why less intrusive alternatives have not been or would not be as effective;
- An assurance that the material obtained will be selected for examination only so far as it is necessary for one or more of the operational purposes specified on the warrant and that it meets the other requirements of section 179 of the Act; and
- An assurance that all material will be kept for no longer than necessary and handled in accordance with the safeguards required by sections 177 of the Act.

Authorisation of a bulk equipment interference warrant

5.10 A bulk equipment interference warrant may only be issued if the Secretary of State considers that the purpose of the warrant is to obtain overseas-related communications, overseas-related information or overseas-related equipment data.

Necessity

5.11 The Secretary of State may only issue a bulk equipment interference warrant if the Secretary of State considers that the warrant is necessary in the interests of national security, or on that ground and for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the UK.

5.12 The power to issue a bulk equipment interference warrant for the purpose of safeguarding the economic well-being of the UK may only be exercised where it appears to the Secretary of State that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant on these grounds if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant for the purpose of safeguarding the economic well-being of the UK should therefore identify the circumstances that are relevant to the interests of national security.

5.13 As set out in section 165(3), the power to issue a bulk equipment interference warrant for the purpose of safeguarding the economic well-being of the UK may also only be exercised in circumstances where the information it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.

5.14 Before issuing a bulk equipment interference warrant, the Secretary of State must also consider that the examination of material obtained under the warrant is necessary for one or more of the specified operational purposes (section 165(1)(d)). Material obtained under the warrant can only be selected for examination when necessary for one of the specified operational purposes. When considering the specified operational purposes, the Secretary of State must also be satisfied that any examination of the material obtained under the warrant for those purposes is necessary for one or more of the statutory purposes set out on the warrant (as at 165(1)(b) and 165(2) and (3)). For example, if a bulk equipment interference warrant is issued in the interests of national security and for the purpose of preventing or detecting serious crime, every specified operational purpose on that warrant must be necessary for one or both of these two broader purposes.

Proportionality

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

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

Safeguards

5.17 Before deciding to issue a warrant, the Secretary of State must consider that satisfactory arrangements are in force in relation to the warrant, setting out the safeguards for the copying, dissemination and retention of intercepted content and secondary data. These safeguards are explained in Chapter 8 of this code.

Authorisation of a bulk equipment interference warrant: senior officials

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

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

Judicial Commissioner Approval

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

5.21 Section 166 of the Act sets out the test that a Judicial Commissioner must apply when deciding whether to approve a bulk equipment interference warrant. The Commissioner must review the Secretary of State's conclusions as to

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

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

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

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

Urgent authorisation of bulk equipment interference warrants

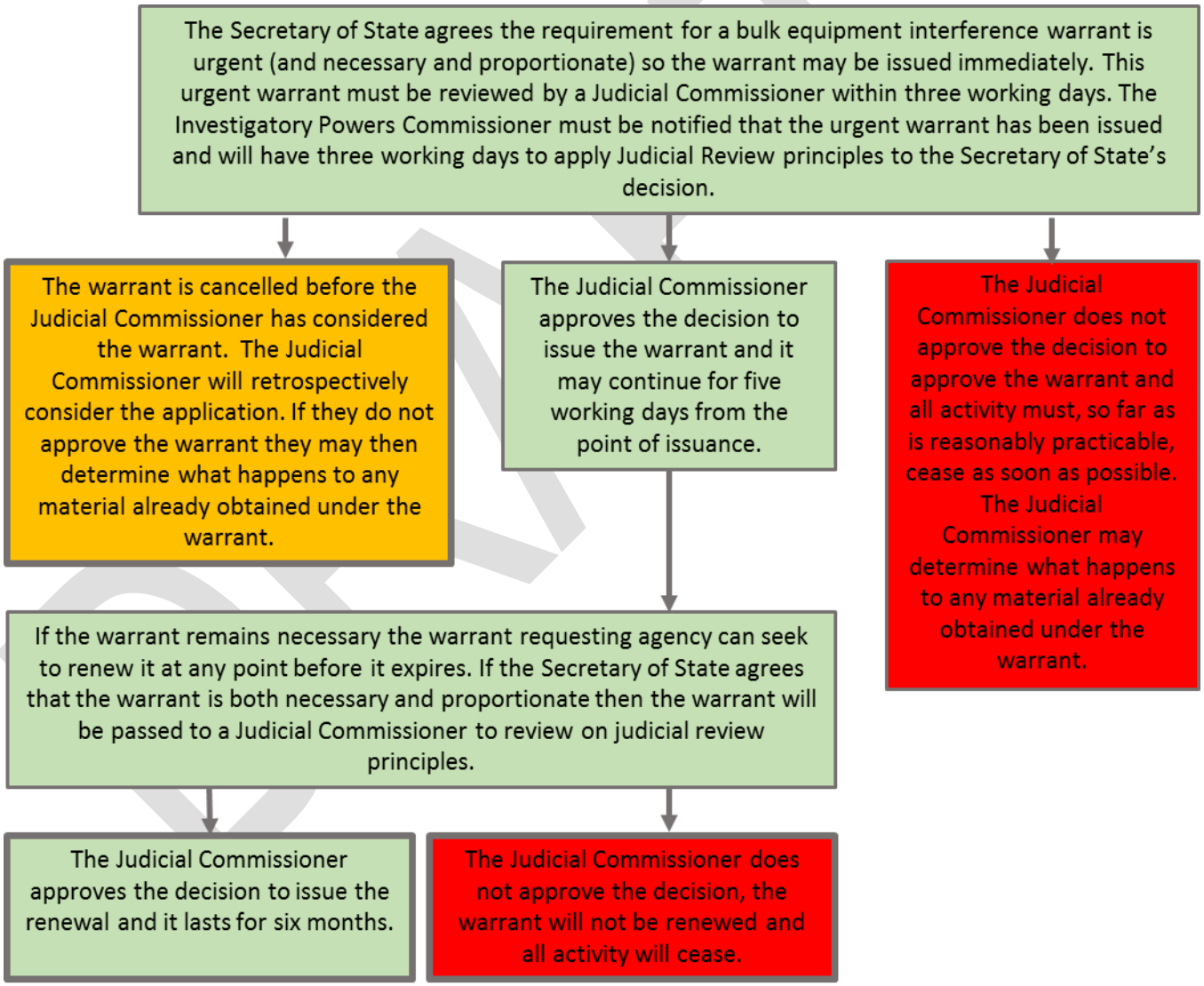
5.24 The Act makes provision for cases in which a bulk equipment interference warrant is required urgently. Urgency is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the requisite time. Accordingly, urgent warrants can permit equipment interference when issued by the issuing authority without prior approval from a Judicial Commissioner. The requisite time would reflect when the authorisation needs to be in place to meet an operational or investigative need. Urgent warrants should fall into at least one of the following three categories:

- Imminent threat to life or serious harm - for example, if there is intelligence to suggest an impending terrorist attack;
- An intelligence gathering opportunity which is significant because of the nature of the potential intelligence, the operational need for the intelligence is significant, or the opportunity to gain the intelligence is rare or fleeting – for example, a group of terrorists is about to meet to make final preparations to travel overseas;
- A significant investigative opportunity - for example, a consignment of weapons is about to enter the UK that the security and intelligence agencies eventually may be used for acts of terror.

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

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

5.27 The following diagram illustrates the bulk equipment interference urgent authorisation process:



Warrants ceasing to have effect and retrieval of equipment

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

5.29 The equipment interference agency may make representations to the Judicial Commissioner about the following matters:

- Whether further equipment interference should be authorised to enable the agency to secure that anything in the process of being done under the warrant stops as soon as possible;
- destruction of any material obtained under the warrant; and
- the conditions that should be imposed as to the use or retention of any of that material.

Format of a bulk equipment interference warrant

5.30 A bulk equipment interference warrant must contain a provision stating that is a bulk equipment interference warrant. Each warrant is addressed to the head of the security and intelligence agency by whom, or on whose behalf, the application was made. Where relevant, a copy may then be served on any person who may be required to provide assistance in giving effect to the warrant. The warrant should include the following:

- A description of the conduct authorised by the warrant;
- The operational purposes for which any material obtained under the warrant may be selected for examination;
- The warrant reference number; and
- Details of the persons who may subsequently modify the operational purposes of a warrant in an urgent case.

Duration of bulk equipment interference warrants

5.31 Bulk equipment interference warrants issued using the standard procedure are valid for an initial period of six months. Warrants issued under the urgency procedure are valid for five working days following the date of issue unless renewed by the Secretary of State. Upon renewal, warrants are valid for a further period of six months. This period begins on the day after the day of which the warrant would have expired, had it not been renewed.

5.32 Where modifications to a bulk equipment interference 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.

Modification of a bulk equipment interference warrant

5.33 A bulk equipment interference warrant may be modified by an instrument under the provisions at section 173 of the Act. The modifications that can be made to a bulk equipment interference warrant are:

- to add, vary or remove an operational purpose specified on the warrant, for which material obtained under the warrant may be selected for examination; and
- to add to, vary or remove any part of the description of the conduct authorised by the warrant.

5.34 In circumstances where a modification is being made to add or vary an operational purpose or any part of the authorised interference, the modification must be made by a Secretary of State and must be approved by a Judicial Commissioner before the modification comes into force. The considerations set out in paragraphs 5.11 - 5.16 apply to a modification as they do to the issuing of a new warrant.

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

5.36 The modification process for bulk equipment interference requires the same level of authorisation as an application for a new bulk equipment interference warrant. When applying to modify an existing warrant, both the warrant applicant and Secretary of State should consider whether the requested modification to the warrant remains within the scope of the original warrant. If the modification is considered to be outside of the scope of the original arrant a new warrant should be sought.

5.37 A bulk equipment interference warrant authorises a two stage process; the acquisition of material, followed by the selection for examination of the material collected under the warrant. There will be limited circumstances where it may no longer be necessary, or possible, to continue the first stage of this process. In such circumstances, it may continue to be necessary and proportionate to select for examination the material collected under that warrant. The Act therefore provides that a bulk equipment interference warrant can be modified such that it no longer authorises the acquisition of material but continues to authorise selection for examination.

Urgent modification of a bulk equipment interference warrant

5.38 Section 174 of the Act makes provision for cases in which modifications of a bulk equipment interference warrant are required urgently. A modification will only be considered urgent if there is a very limited window of opportunity to act, as described in paragraph 4.504.50 of this code. The modifications that can be made urgently to a bulk equipment interference warrant are:

- to add or vary or remove an operational purpose specified on the warrant, for which material obtained under the warrant may be selected for examination; and
- to add to or vary or remove any part of the description of the conduct described in the equipment warrant.

5.39 In these cases the Secretary of State may make the urgent modification but it must be reviewed by a judicial commissioner within five working days. The Secretary of State must personally authorise the modification. Where possible, the Secretary of State will also sign the modification instrument. If this is not possible, the modification instrument may be signed by a senior official after the case, including considerations of necessity and proportionality, has been considered and approved by the Secretary of State. The Act restricts urgent modifications to bulk equipment interference warrants in this way to cases where the Secretary of State has expressly authorised the issuing of the warrant and requires the warrant to contain a statement to that effect.

5.40 In the event that the judicial commissioner does not agree to the urgent modification, the activity conducted under the urgent modification remains lawful. The judicial commissioner may authorise further interference, but only in the interest of ensuring that anything being done by virtue of the modification is stopped as soon as possible.

5.41 The urgent modification will only last for a maximum of five working days following its implementation unless renewed. If it is renewed it expires after six months, in the same way as non-urgent modifications of targeted equipment interference warrants.

Renewal of a bulk equipment interference warrant

5.42 The Secretary of State may renew a bulk equipment interference warrant at any point before its expiry date (section 172 of the Act). Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 5.9 above. In particular, the applicant must give an assessment of the value of the equipment interference to date and explain why it is considered that the interference continues to be necessary in the interests of national security as well as, where applicable, either or both of the purposes in section 165(2), and why it is considered that the conduct authorised by the warrant continues to be proportionate.

5.43 In deciding to renew a bulk equipment interference warrant, the Secretary of State must also consider that the examination of material obtained under it continues to be necessary for one or more of the specified operational purposes, and that any examination of that material for these purposes is necessary for one or more of the statutory purposes on the warrant.

5.44 In the case of a renewal of a bulk equipment interference warrant that has been modified so that it no longer authorises or requires the acquisition of material, it is not necessary for the Secretary of State to consider that the acquisition of such material continues to be necessary before making a decision to renew the warrant.

5.45 Where the Secretary of State is satisfied that the warrant continues to meet the requirements of the Act, the Secretary of State may renew it. The renewed warrant is valid for six months from the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed. For example, where a warrant is due to expire on 1 January, and the Secretary of State and Judicial Commissioner are satisfied that it should be renewed, the renewed warrant will be expire on 2 July.

5.46 In those circumstances where the assistance of a CSP or other person 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

5.47 The Secretary of State, or a senior official acting on their behalf, may cancel a bulk equipment interference warrant at any time. Such persons must cancel a warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary in the interests of national security or the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct. Such persons must also cancel a warrant if, at any time before its expiry date, he or she is satisfied that the examination of material acquired under the warrant is no longer necessary for any of the operational purposes specified on the warrant.

5.48 Equipment interference agencies will therefore need to keep their warrants under regular review and must notify the Secretary of State if they assess that the equipment interference 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.

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

5.50 The cancellation instrument will be addressed to the equipment interference agency to whom the warrant was issued. A copy of the cancellation instrument should be sent to those providers or other persons, if any, who have given effect to the warrant during the preceding twelve months.

Examination Safeguards

Safeguards when selecting for examination content obtained under a bulk equipment interference warrant

5.51 Section 179 of the Act provides specific safeguards relating to the selection for examination of material acquired under a bulk equipment interference warrant. References to examination of material are references to it being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.

5.52 Sections 179(1) and (2) make clear that selection for examination may only take place for one or more of the operational purposes that are specified on the warrant. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination, rather than limiting the information which can be examined per se, and no official is permitted to gain access to the data other than as permitted by these purposes. Material selected for examination for an operational purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained on any relevant ground.

5.53 Section 179 makes clear that operational purposes must relate to one or more of the statutory purposes specified on the warrant. However, it is not sufficient under the Act for operational purposes simply to use the wording of one of the statutory purposes. They must include more detail to ensure that material can only be selected for examination for specific reasons. Operational purposes provide the Secretary of State and the Judicial Commissioner with a more granular understanding of the purposes for which the material will be selected for examination.

5.54 Although bulk equipment interference warrants are authorised for the purpose of acquiring overseas-related communications, equipment data or other information, section 179(5) of the Act makes clear that a bulk equipment interference warrant can authorise the acquisition of material that is not overseas-related to the extent this is necessary in order to acquire the overseas-related material to which the warrant relates. Operational purposes specified on bulk equipment interference warrants may therefore include purposes that enable the selection for examination of material of individuals in the UK. The safeguards in section 179 of the Act ensure that where protected material is selected for examination by any criteria referable to an individual known to be in the British Islands at that time, a targeted examination warrant must be obtained under Part 5 of the Act authorising the selection for examination of that material.

5.55 The security and intelligence agencies need to retain the operational agility to respond to developing and changing threats and the range of operational purposes that may need to be specified on a bulk warrant needs to reflect this. New operational purposes will therefore be required over time. The Act provides for a bulk equipment interference warrant to be modified such that the operational purposes specified on it can be added to or varied by the Secretary of State with approval from a Judicial Commissioner. In addition, a senior official may modify a bulk equipment interference warrant to remove one or more operational purposes.

5.56 In line with this, the security and intelligence agencies will need to ensure the full range of their bulk warrants are relevant to the current threat picture and, where applicable, the intelligence priorities set by the National Security Council. They will need to identify operational purposes that need to be added to or removed from bulk warrants, including in urgent circumstances. This would be done through the modifications process set out at Section 173 of the Act.

5.57 Some operational purposes that may need to be specified on a bulk warrant will be consistent across the three agencies, although some purposes will be relevant to a particular agency or two of the three, reflecting differences in their statutory functions. Operational purposes should as far as possible be consistent across the bulk capabilities provided for by the Act.

5.58 As well as being necessary for one of the operational purposes, any selection for examination of material must be necessary and proportionate.

5.59 In general, automated systems must, where technically possible, be used to effect the selection in accordance with section 179 of the Act. As an exception, material acquired through bulk equipment interference may be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the content falls within the main categories to be selected under the specified operational purposes, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary on the grounds specified in sections 165(1)(b) and 165(2) of the Act. Once those functions have been fulfilled, any copies made of the content for those purposes must be destroyed in accordance with section 177(5) of the Act. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the IPC during his or her inspections.

5.60 Communications and information collected under a bulk equipment interference warrant should be selected for examination only by authorised persons who receive mandatory training regarding the provisions of the Act and specifically the operation of section 179 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.

5.61 Prior to an authorised person being able to select for examination, a record should be created setting out why access to the content is necessary in pursuance of section 179 and the applicable operational purpose(s), and why such access is proportionate. Save where the content or automated systems are being checked as described in paragraph 5.59, the record must indicate, by reference to specific factors, the content to which access is being sought and systems should, to the extent possible, prevent access to the content unless such a record has been created. Where it is anticipated that the selection for examination is likely to give rise to collateral intrusion into privacy, the reasons this is considered proportionate, and any steps to minimise it, must also be recorded. All records must be retained in accordance with agreed policy for the purposes of subsequent examination or audit.

5.62 Access to the content as described in paragraph 5.61 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.

5.63 Periodic audits should be carried out to ensure that the requirements set out in section 179 of the Act are being met. These audits must include checks to ensure that the records requesting selection for examination have been correctly compiled, and specifically, that the content requested falls within operational purposes the Secretary of State has considered necessary for examination. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards must be reported to the IPC. All intelligence reports generated by the authorised persons must be subject to a quality control audit.

5.64 The Secretary of State must ensure that the safeguards are in force before any interference under a bulk equipment interference warrant can begin. The IPC is under a duty to review the adequacy of the safeguards.

5.65 More than one operational purpose may be specified on a single bulk warrant; this may, where the necessity and proportionality test is satisfied, include all the operational purposes currently specified on the central list maintained by the heads of the security and intelligence agencies.

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

Selection for examination of protected material in breach of the section 179(4) prohibition

5.67 Any selection for examination of protected material must also meet the selection conditions set out at section 179(3) and (4). Section 179(4) prohibits the selection of protected material for examination using criteria referable to an individual known to be in the British Islands in order to identify the content of communications content or private information of that individual. Selection in breach of this prohibition is only permitted where:

- A targeted examination warrant has been issued under Part 5 authorising the examination of the protected material, or
- The selection for examination in breach of the prohibition is authorised by section 170(5).

5.68 Selection in breach of the prohibition in section 179(4) of the Act may be authorised by section 179(5) authorisation. Subsection (5) addresses cases where there is a change of circumstances such that a person whose material is being selected for examination enters or is discovered to be in the British Islands, for example where a member of an international terrorist or organised crime group travels into the UK. To enable the selection for examination to continue, sections 179(5) and 179(6) of the Act provide for a senior official to give a written authorisation for the continued selection for examination of protected material relating to that person for a period of five working days. Any selection for examination after that point will require the issue of a targeted examination warrant, issued by the Secretary of State and approved by a Judicial Commissioner. Where selection for examination is undertaken in accordance with section 179(5), the Secretary of State must be notified.

6 Implementation of warrants and Communication Service Provider compliance

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

6.2 Section 121 of the Act permits a number of equipment interference agencies to serve a warrant on telecommunication operators. The agencies named by the Act are:

- The Security and Intelligence Agencies;
- Defence intelligence;
- The NCA;
- The Metropolitan Police Service;
- The Police Service of Scotland;
- The Police Service of Northern Ireland; and
- Her Majesty's Revenue and Customs.

6.3 Where a copy of an equipment interference warrant has been served on anyone providing a 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. For the purpose of requiring any person to provide such assistance, the equipment interference agency may serve a copy of the warrant on any person, inside or outside the UK, who is required to provide assistance in relation to that warrant[21].

6.4 Section 120 of the Act[22] provides that service of a copy of a warrant on a person outside the UK may (in addition to electronic or other means of service) be effected in any of the following ways:

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

[21] See section 121 of the Act.

[22] By virtue of section 176 of the Act, section 120 (service of warrants) applies in relation to bulk equipment interference warrants as it applies in relation to targeted warrants.

Provision of reasonable assistance to give effect to a warrant

6.5 Any CSP, or any person who offers or provides a telecommunications service to the UK or has control of a telecommunications system located wholly or partly in the UK, may be required to provide assistance in giving effect to an equipment interference warrant. A warrant can only be served on a person who is considered by the implementing authority to be able to provide the assistance required by the warrant. . For the avoidance of doubt, in appropriate circumstances, this does not prevent equipment interference agencies and providers working co-operatively together (without the need for service of a copy of an equipment interference warrant in accordance with section 121).

6.6 In the case of the Security and Intelligence Agencies and Defence Intelligence, the Act places a requirement on providers served with a warrant, issued by the Secretary of State or the Scottish Ministers, to take all reasonably practicable steps for giving effect to the warrant as are notified to them (section 121(5)).

6.7 In the case of warrants issued to specified law enforcement officers, the Act places a requirement on providers to take all such steps for giving effect to the warrant as were approved by the Secretary of State and as are notified to the provider by or on behalf of the law enforcement officer to whom the warrant is addressed (section 121(2)). Section 121(2) and (4) ensures that the steps that providers are required to take are limited to those that the Secretary of State has expressly approved as necessary and proportionate to what is sought to be achieved by them. Equipment interference agencies should endeavour to work co-operatively with persons providing assistance in giving effect to warrants, and should seek to implement warrants on a collaborative basis. Assistance sought will typically comprise (but may not be limited to) the provision of infrastructure by a relevant CSP, or details about the technical specification of relevant equipment.

6.8 When requesting assistance that would involve employees of a telecommunication service provider, the equipment interference agency and the Secretary of State should consider during the authorisation process:

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

6.9 In some cases equipment interference agencies may consider that the same material can be acquired either with assistance of a CSP or independently. The agency and issuing authority should consider the merits of either approach in the context of the specific operation, this should include the consideration of the criteria in paragraph 3.27.

6.10 The steps which may be required by CSPs are limited to those which it is reasonably practicable to take (section 121(5)). What is reasonably practicable will be considered on a case-by-case basis, taking into account the individual circumstances of the relevant CSP, and should be agreed after consultation between the CSP and the Government. Such consultation is likely to include consideration of a number of factors including, but not limited to, the technical feasibility and likely cost of complying with any steps notified to the CSP. As part of the consultation, the CSP may raise any other factor that they consider relevant to whether the taking of such steps is reasonably practicable. If no agreement can be reached it will be for the Secretary of State to decide whether to proceed with civil proceedings.

6.11 Where the equipment interference agency requires the assistance of a CSP in order to implement a warrant, it must provide one or more of the following to the CSP:

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

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

6.13 Section 94(5)(b) of the Act makes lawful any conduct undertaken by a person in pursuance of requirements imposed by or on behalf of a person to whom an equipment interference warrant is addressed. This therefore authorises activity taken by CSPs in giving effect to a warrant that would otherwise constitute an offence under the CMA, Data Protection legislation or other relevant legislation. Where assistance is required that - but for section 94(5)(b) - would constitute an offence, the issuing authority and, if not the issuing authority, the Secretary of State should consider ways in which the warrant can be executed so as to minimise such activity and the need to rely on section 94(5)(b); this is part of the consideration of whether the activity authorised by the warrant is proportionate and cannot be achieved by less intrusive means

Contribution of costs for giving effect to an equipment interference warrant

6.14 Section 225 of the Act recognises that CSPs incur expenses in complying with requirements in the Act, including equipment interference in response to requests under Part 5 of the Act. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.

6.15 Public funding and support is made available to CSPs to ensure that they can provide, outside of their normal business practices, an effective and efficient response to public authorities' necessary, proportionate and lawful requirements in support of their investigations and operations in the interests of national security, to protect the public and to bring to justice those who commit crime.

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

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

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

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

7 Maintenance of a technical capability

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

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

7.3 The obligations that the Secretary of State considers reasonable to impose on CSPs are set out in regulations made by the Secretary of State and approved by Parliament, and may include (amongst others) obligations set out at section 229(4) of the Act:

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

7.4 An obligation placed on a CSP to remove encryption only relates to electronic protections that the company has itself applied to material (and secondary data), or where those protections have been placed on behalf of that CSP. The purpose of this obligation is to ensure that the requested material can be provided to the equipment interference agencies in readable form. References to protections applied on behalf of the CSP include circumstances where the CSP has contracted a third party to apply electronic protections to a telecommunications service provided by that CSP to their customers.

7.5 In the event that a number of CSPs are involved in the provision of a service, the obligation to provide a capability, and to remove encryption, will be placed on the CSP which has the technical capability to give effect to the notice and on whom it is reasonable practicable to impose these requirements. It is possible that more than one CSP will be involved in the provision of the capability, particularly if more than one CSP applies electronic protections to the relevant material.

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

Consultation with service providers

7.7 Before giving a notice, the Secretary of State must consult the CSP[23]. In practice, informal consultation is likely to take place long before a notice is given. The Government will engage with CSPs who are likely to be subject to a notice in order to provide advice and guidance, and prepare them for the possibility of receiving a notice.

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

Matters to be considered by the Secretary of State

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

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

- The likely benefits of the notice – this may take into account projected as well as existing benefits.
- The likely number of users (if known) of any service to which the notice relates – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the technical capability notice.
- The technical feasibility of complying with the notice – taking into account any representations made by the CSP and giving specific consideration to any obligations in the notice to remove electronic protections (as described at 231(4)).
- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the CSP as part of the notice, such as those relating to security. This should also include specific consideration to the likely cost of complying with any obligations in the notice to remove electronic protections. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money.
- Any other effect of the notice on the CSP – again taking into account any representations made by the company.

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

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means,
- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.

[23] See section 218(2).

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

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

Giving a notice

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

7.15 Section 229(8) provides that obligations may be imposed on, and technical capability notices given to, persons located outside the UK and may require things to be done or not done outside the UK. Where a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given to the CSP[24]:

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

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

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

7.18 A person to whom a technical capability notice is given is under a duty to comply with the notice. In respect of a technical capability notice to give effect to equipment interference warrants, the duty to comply with a technical capability notice is enforceable against a person in the UK by civil proceedings by the Secretary of State[25]. The duty to comply with a technical capability notice to give effect to equipment interference warrants is enforceable against a person in the UK and a person outside the UK by civil proceedings by the Secretary of State[26].

[24] See section 231(6).

[25] See section 231(10)(a).

[26] See section 231(10)(b).

Disclosure of technical capability notices

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

7.20 Any person to whom a technical capability notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence and contents of that notice to any person[27].

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

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

7.22 Section 125 of the Act sets out the meaning of “excepted disclosure” and the circumstances in which disclosure made in relation to a warrant is permitted. This includes when a disclosure is made, not in relation to a particular warrant but in relation to equipment interference warrants in general. This includes provision for CSPs to be able to publish information in relation to the number of warrants they have given effect to. In order to ensure that this does not reveal sensitive information that could undermine the ability of the security and intelligence and law enforcement agencies to do their job, further information on the way in which this information can be published is set out in regulations. The regulations make clear that statistical information can be published on the number of warrants that a CSP has given effect to within a specified range rather than the exact number.

Regular review

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

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

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

[27] See section 218(8).

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

- a significant change in demands by the equipment interference agencies that calls into question the necessity and proportionality of the notice as a whole, or any element of the notice;
- a significant change in the CSP's activities or services; or
- a significant refresh or update of CSP's systems.

7.27 The process for reviewing a notice requires the Secretary of State to consult the CSP to determine whether the notice remains necessary and proportionate.

7.28 A review may recommend the continuation, variation or revocation of a notice. The relevant CSP and the equipment interference agencies will be notified of the outcome of the review.

Variation of technical capability notices

7.29 The communications market is constantly evolving and CSPs subject to technical capability notices will often launch new services.

7.30 CSPs subject to a technical capability notice must notify the Government of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require the CSP to provide a technical capability on the new service.

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

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

- a CSP launching new services;
- changing law enforcement demands and priorities;
- a recommendation following a review (see paragraph 7.28 above); or
- to amend or enhance the security requirements.

7.33 Where a CSP has changed name, for example as part of a rebranding exercise or due to a change of ownership, the Secretary of State, in consultation with the CSP, will need to consider whether the existing notice should be varied.

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

7.35 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraph 7.7.

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

Revocation of technical capability notices

7.37 A technical capability notice must be revoked (in whole or in part) if it is no longer necessary or proportionate to require a CSP to provide a technical capability.

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

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

Referral of technical capability notices

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

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

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

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

7.44 After considering reports from the TAB and the Commissioner, the Secretary of State may decide to vary, withdraw or confirm the effect of the notice. Where the Secretary of State decides to confirm or vary the notice, the Investigatory Powers Commissioner must approve the decision. Until the Secretary of State's decision is approved, there is no requirement for the CSP to comply with the notice so far as referred. The CSP will remain under obligation to provide assistance in giving effect to an equipment interference warrant, as set out in section 121 of the Act.

Contribution of costs for the maintenance of a technical capability

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

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

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

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

7.49 Contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the use of such services. However, where a CSP expands or changes its network for commercial reasons, it is expected to meet any capital costs that arise.

General considerations on appropriate contributions

7.50 Any CSP seeking to recover appropriate contributions towards its costs should make available to the Government such information as the Government requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the CSP.

7.51 As costs are reimbursed from public funds, CSPs should take into account value for money when procuring, operating and maintaining the infrastructure required to comply with a notice. As changes to business systems may necessitate changes to systems, CSPs should take this into account when altering business systems and must notify the Government of proposed changes.

7.52 Any CSP that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made. This is to ensure that expenditure has been incurred for the stated purpose. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

Power to develop compliance systems

7.53 In certain circumstances it may be more economical for products to be developed centrally, rather than CSPs or public authorities creating multiple different systems to achieve the same end. Where multiple different systems exist, it can lead to increased complexity, delays and higher costs when updating systems (for example, security updates).

7.54 Section 226 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop consistent systems for use by CSPs to acquire material. Such systems could operate in respect of multiple powers under the Act.

7.55 Where such systems are developed for use by CSPs, the Government will work closely with CSPs to ensure the systems can be properly integrated into their networks. CSPs using such systems will have full sight of any access or processing of their data carried out by such systems.

Principles of data security, integrity and disposal of systems

Legal and regulatory compliance

7.56 All equipment interference systems and practices must be compliant with relevant legislation.

7.57 All systems and practices must comply with any security policies and standards in place in relation to equipment interference. This may include any policies and standards issued by the Home Office. These further requirements are unlikely to be publicly available as they may contain specific details of security infrastructure or practices, disclosure of which could create additional security risks.

Information security policy & risk management

7.58 Each communications service provider must develop a security policy. This policy document should describe the internal security organisation, the governance and authorisation processes, access controls, necessary training, the allocation of security responsibilities, and policies relating to the security and integrity of capabilities. Each communications service provider must also develop security operating procedures. A communications service provider can determine whether this forms part of, or is additional to, wider company policies.

7.59 The security policy document and security operating procedures should be reviewed regularly to ensure they remain appropriate

7.60 Each communications service provider must identify, assess and treat all information security risks, including those which relate to arrangements with external parties.

Human Resources Security

7.61 Communications service providers must clearly identify roles and responsibilities of staff, ensuring that roles are appropriately segregated to ensure staff only have access to the information necessary to complete their role. Access rights and permissions assigned to users must be revoked on termination of their employment. Such rights and permissions must be reviewed and, if appropriate, amended or revoked when staff move roles within the organisation.

7.62 Staff with access to sensitive systems and sensitive information related to warranted interference should be subject to an appropriate level of security screening. The Government sponsors and manages security clearance for certain staff working within a communications service provider to ensure the company's compliance with obligations under this legislation. Communications service providers must ensure that these staff have undergone relevant security training and have access to security awareness information.

7.63 All persons who may have access to the product of equipment interference, 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.

7.64 Where it is necessary for an officer of an equipment interference agency to disclose information related to warranted equipment interference to a communications service provider operating under a technical capability notice, it is the former's responsibility to ensure that the recipient has the necessary security clearance.

Maintenance of Physical Security

7.65 There should be appropriate security controls in place to prevent unauthorised access to sensitive information. Access to the locations where the systems are both operated and hosted must be controlled such that access is limited to those with the relevant security clearance and permissions.

7.66 Equipment used to for the purpose of warranted equipment interference must be sanitised and securely disposed of at the end of its life[28].

Operations management

7.67 Systems used for equipment interference should be subject to a documented change management process, including changes to third party suppliers, to ensure that no changes are made to systems without assessing the impact on the security of the product.

7.68 Communications service providers must also put in place a patching policy to ensure that regular patches and updates are applied to any equipment interference capabilities or support systems as appropriate. Such patches and updates will include anti-virus, operating systems, application and firmware. The patching policy including timescale in which patches must be applied, must be agreed with the Home Office.

7.69 Communications service providers should ensure that, where encryption is in place in equipment interference systems, any encryption keys are subject to appropriate controls, in accordance with the appropriate security policy.

7.70 Network infrastructure, services, media, and system documentation must be stored and managed in accordance with the security policy and an inventory of all assets should be maintained together with a clear identification of their value and ownership. All assets must be clearly labelled.

Access Controls

7.71 Where a communication service provide has access to any equipment that forms part of a technical capability, they must ensure that registration and access rights, passwords and privileges for access to dedicated equipment interference systems and associated documentation are managed in accordance with their security policy. They must also ensure that users understand and formally acknowledge their security responsibilities.

7.72 Access to operating systems must be locked down to an appropriate standard and any mobile computing (i.e. offsite access to communications service provider systems from non-secure locations) must be subject to appropriate policies and procedures if permitted. Accordingly any remote access for diagnostic, configuration and support purposes must be controlled.

7.73 Access should be provided to relevant oversight bodies where necessary for them to carry out their functions.

Additional requirements relating to the disposal of systems

7.74 The legal requirement to ensure deleted data is impossible to access must be taken into account when disposing of any system, or component of a system, which reaches the end of its service life.

[28] Please see 8.91 for further details on the disposal of equipment interference systems.

7.75 If the equipment is to be re-used, it must be securely sanitised by means of overwriting using a Government-approved product. If the equipment is not to be re-used immediately, it must be securely stored in such a way that it may only be re-used or disposed of appropriately.

7.76 If the equipment is to be finally disposed of, it must be securely sanitised by means of physical destruction by a Government-approved supplier.

7.77 Sanitisation or destruction of information used to identify relevant equipment must include retained copies for back-up and recovery, and anything else that stores duplicate data within the communications service provider's system, unless retention of this is otherwise authorised by law.

8 Handling of information, general safeguards and sensitive professions

Overview

8.1 This chapter provides general guidance on the processing, retention, disclosure, deletion and destruction of all material obtained by the equipment interference agencies pursuant to all equipment interference warrants. The additional safeguards which apply to the examination of such material obtained under a bulk equipment interference warrant are explained in chapter 6 of this code.

8.2 All material obtained under the authority of an equipment interference warrant must be handled in accordance with safeguards which the Secretary of State, Scottish Minister or law enforcement chief considers to be satisfactory[29]. These safeguards are made available to the IPC, and they must meet the requirements of sections 122 and 177 of the Act which are set out below. In addition, the safeguards in 179 apply to the selection for examination of material obtained under bulk equipment interference warrants. Any breach of these safeguards must be reported to the IPC. The equipment interference 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.

8.3 In any case where communications, equipment data or other information are obtained under sections 5 or 7 of the 1994 Act or Part 3 of the 1997 Act, equipment interference agencies must handle the material so obtained in accordance with the safeguards set out in Covert Surveillance and Property Interference Code. Compliance with these safeguards will ensure that the relevant service handles the material in accordance with safeguards equivalent to those set out in chapter 8 of this code[30].

Use of material as evidence

8.4 Subject to the provisions in chapter 8 of this code, material obtained through equipment interference may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996, the Criminal Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984[31] and the Human Rights Act 1998.

[29] Before issuing a targeted or bulk equipment interference warrant, the issuing authority must be satisfied that such arrangements are in force in relation to the warrant: see sections 97(1)(c) and 1657(1)(e).

[30] The Covert Surveillance and Property Interference Code will be updated prior to implementation of the Act.

[31] And section 76 of the Police and Criminal Evidence (Northern Ireland) Order 1989.

8.5 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure test applied under the Criminal Procedure and Investigations Act 1996 and these considerations will apply to any material acquired through equipment interference that is used in evidence'. When information obtained from equipment interference is used evidentially, the equipment interference agency should be able to demonstrate how the evidence has been recovered, and be capable of showing each process through which the evidence was obtained where appropriate to do so.

8.6 Where the product of equipment interference could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review. In the cases of the law enforcement equipment interference agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996.

8.7 The heads of the Security and Intelligence Agencies and law enforcement agencies are also under a duty to ensure that arrangements are in force to secure: (i) that no information is obtained except so far as necessary for the proper discharge of their functions; and (ii) that no information is disclosed except so far as is necessary for those functions, for the purpose of any criminal proceedings, and, in the case of SIS and the Security Service, for the other purposes specified. In the case of the Security and Intelligence Agencies the arrangements must include provision with respect to the disclosure of information obtained by virtue of sections 5 and 7 of the 1994 Act, and any information so obtained must be subject to the arrangements.

General safeguards

8.8 Sections 122 and 177 of the Act require that disclosure, copying and retention of material obtained under equipment interference warrants is limited to the minimum necessary for the authorised purposes. Something is necessary for the authorised purposes if the material:

- Is, or is likely to become, necessary on any relevant grounds as set out in section 122(7) or for any of the purposes set out in sections 165(2) – as relevant, in the interests of national security, for the purpose of preventing or detecting serious crime, for the prevention of death or injury, 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[32];
- Is necessary for facilitating the carrying out of the functions under the Act of the issuing authority or the person to whom the warrant is addressed;
- Is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal;
- Is necessary for the purposes of legal proceedings; or
- Is necessary for the performance of the functions of any person by or under any enactment.

[32] Material obtained for one purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained for another.

8.9 For the avoidance of doubt, when a security and intelligence agency obtains material under a bulk equipment interference warrant and selects for examination that material in accordance with the specified operational purposes, the selected material may be retained, copied, processed and disseminated on any relevant ground.

Reviewing warrants

8.10 Regular reviews of all warrants should be undertaken during their currency to assess the need for the equipment interference activity to continue. The results of a review should be retained for at least three years. Particular attention should be given to the need to review warrants frequently where the equipment interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

8.11 In each case, unless specified by the issuing authority or Judicial Commissioner, the frequency of reviews should be determined by the equipment interference agency who made the application. This should be as frequently as is considered necessary and proportionate.

8.12 In the event that there are any significant and substantive changes to the nature of the interference and/or the identity of the equipment during the currency of the warrant, the equipment interference agency should consider whether it is necessary to apply for a fresh warrant.

Dissemination of material obtained under an equipment interference warrant

8.13 The number of persons to whom any of the material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. In the same way, only so much of the material may be disclosed as is necessary for the authorised purposes. For example, if a summary of the material will suffice, no more than that should be disclosed.

8.14 The obligations apply not just to the original agency who obtained the data, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

8.15 Sections 123 and 178 of the Act provide that where material obtained under an equipment interference warrant, or a copy of such material, is handed over to the authorities of a country or territory outside the UK, the issuing authority must ensure that arrangements are in force to ensure that the material is only shared if the UK agency considers that arrangements corresponding to the requirements in sections 122 and 177 (relating to minimising the extent to which material is disclosed, copied, distributed and retained) will apply to the extent that the UK agency considers appropriate. In particular, the material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed.

Offence of making unauthorised disclosure

8.16 According to section 126 of the Act it is a criminal offence to make unauthorised disclosure of the existence, content or details relating to an equipment interference warrant, the existence of content of any requirement to provide assistance in giving effect to a warrant, any steps taken in pursuance of a warrant and any material derived from equipment interference. This offence applies to all parties listed in section 124 (3). The offence does not apply however if:

- The disclosure is an excepted disclosure according to section 125. For example, a law enforcement officer may be authorised by the person to whom an equipment interference warrant is addressed to disclose material acquired by equipment interference in order to carry out their functions; or
- The offence does not apply to individuals who are unaware that the disclosure of the material in question would be in breach of the duty not to make unauthorised disclosures. This could be because they are not aware that the material they are disclosing is derived from equipment interference, as it may not be identifiable as the product of equipment interference.

8.17 Section 125 (2) sets out that disclosures may be authorised by the warrant, by the person to whom the warrant is addressed or by the terms of any requirement to provide assistance in giving effect to a warrant. If the issuing authority or the person to whom the warrant is addressed intends to authorise a disclosure under this section they must first consider the safeguards set out in section 122 of the Act and paragraphs 8.13 to 8.15 of this Code.

Copying

8.18 Material may only be copied to the extent necessary for the authorised purposes. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of an equipment interference warrant, and any record which includes the identities of the persons who owned, used or were in possession of the equipment interfered with under the warrant.

Storage

8.19 Material and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. This requirement to store material securely applies to all those who are responsible for handling it, including providers. The details of what such a requirement will mean in practice for providers will be set out in the discussions they have with the Government before a technical capability notice for equipment interference is given to a person (see chapter 6 of this code).

Destruction

8.20 Material, and all copies, extracts and summaries which can be identified as the product of an equipment interference warrant, must be marked for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes.

8.21 If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid for one or more of the authorised purposes.

8.22 Any collateral material that has been acquired over the course of a testing or training exercise should be destroyed as soon as reasonably possible following the conclusion of the testing or training.

Safeguards applicable to the handling of material obtained as a result of a request for assistance

8.23 Where material is obtained by a UK equipment interference agency as a result of a request to an international partner to undertake equipment interference on its behalf, the material must be subject to the same internal rules and safeguards that apply to the same categories of material when they are obtained directly by the equipment interference agency as a result of equipment interference under the Act.

Confidential information

8.24 Particular consideration should be given in cases where material is obtained or examined under an equipment interference warrant and the subject of the obtaining or examination might reasonably assume a high degree of privacy, or where confidential information is involved. This includes where the material is legally privileged; where confidential journalistic material may be involved; where equipment interference might involve material relating to communications between a medical professional or Minister of Religion and an individual concerning the latter's health or spiritual welfare; or where material concerning communications between a Member of Parliament and another person on constituency business may be involved.

8.25 Section 106 of the Act provides additional protection for members of relevant legislatures, including Members of Parliament. The Prime Minister must approve any application where it is intended to issue a targeted equipment interference warrant or a targeted examination warrant where the purpose (or one of the purposes) of the warrant is to obtain the communications or private information of a member of a relevant legislature, apart from those approved by Scottish Ministers. The PM must also be consulted before a decision is made to renew a warrant (section 106 of the Act) and prior to making a modification of a warrant in respect of a member of a relevant legislature (section 113(3) of the Act). In a case where section 106 applies in relation to making a modification, the warrant must be approved by a Judicial Commissioner. The Prime Minister must also explicitly authorise any decision made to renew such a warrant (section 110(10) of the Act).

Material involving confidential journalistic material, confidential personal information and exchanges between a Member of Parliament and another person on constituency business

8.26 Particular consideration must also be given to cases where equipment interference includes the obtaining or the examination of material that involves confidential journalistic material, confidential personal information, or communications between a Member of Parliament and another person on constituency business.

8.27 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 material being acquired for the purposes of journalism and held subject to such an undertaking.

8.28 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.

8.29 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.

8.30 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 equipment interference agency.

8.31 Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes. It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.

8.32 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 equipment interference agency and before any further dissemination of the material takes place.

8.33 Any case where confidential information is retained should be notified to the IPC 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.

8.34 The safeguards set out in chapter 8 also apply to any material obtained under a bulk equipment interference warrant which is selected for examination (other than as authorised by a targeted examination warrant) and which constitutes confidential information.

Items subject to legal privilege

8.35 Section 98 of the 1997 Act 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.

8.36 Legal privilege does not apply to material held with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged items will lose its protection if, for example, the professional legal adviser is intending to hold or use the items for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

8.37 For the purposes of this code, any communication between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the items do not form part of a professional consultation of the lawyer, or there is clear and compelling evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the items are subject to legal privilege or over whether the items are not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from a legal adviser within the relevant equipment interference agency.

8.38 Sections 107 and 180 of the Act provides special protections for legally privileged items. Acquiring such items (or examining items subject to legal privilege acquired under a bulk equipment interference 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 acquisition of items subject to legal privilege (whether deliberately obtained or otherwise) is therefore subject to additional safeguards under this code as set out from paragraph 8.35. The guidance set out may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to other content which has been sought.

8.39 In a case where section 107 applies in relation to making a modification, the warrant must be approved by a Judicial Commissioner

Application process for targeted equipment interference and examination warrants

8.40 Where a targeted equipment interference warrant or targeted examination warrant is likely to result in a person acquiring items subject to legal privilege, the application should include, in addition to the reasons why it is considered necessary for the interference or examination to take place, an assessment of how likely it is that items which are subject to legal privilege will be obtained or examined. In addition, it should state whether the purpose (or one of the purposes) of the interference or examination is to obtain privileged items. Where the intention is not to acquire items subject to legal privilege, but it is likely that such items will nevertheless be acquired, that should be made clear in the warrant application and the relevant agency should confirm that any inadvertently obtained items that are subject to legal privilege will be treated in accordance with the safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to the items subject to legal privilege.

8.41 Where the intention is to acquire legally privileged items, the issuing authority will only issue the warrant 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 interference or examination is reasonably regarded as likely to yield intelligence necessary to counter the threat.

Example: An intelligence agency may need to deliberately target legally privileged communications where the legal consultation might yield intelligence that could prevent harm to a potential victim or victims. For example, if they have intelligence to suggest that an individual is about to conduct a

terrorist attack and the consultation may reveal information that could assist in averting the attack (e.g. by revealing details about the location and movements of the individual) then they might want to target the legally privileged communications.

8.42 Further, in considering any such application, the issuing authority must believe that the proposed conduct is proportionate to what is sought to be achieved. In particular the issuing authority must consider whether the purpose of the proposed interference or examination could be served by obtaining non-privileged items. In such circumstances, the issuing authority 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.

8.43 Where there is a renewal application in respect of a warrant which has resulted in the obtaining of legally privileged items, that fact should be highlighted in the renewal application.

Selection for examination of legally privileged protected material under a bulk equipment warrant: requirement for prior approval by independent senior official

8.44 Where protected material obtained under a bulk equipment interference warrant is to be selected for examination according to a factor that is intended, or is likely to, result in a person acquiring items subject to legal privilege, and the selection would not breach the prohibition in section 179(4) (so a targeted examination warrant is not required), the enhanced procedure described at paragraph 8.40 and 8.43 applies.

8.45 An authorised person[33] in a public authority must notify a senior official[34] before using a factor to select any protected material for examination, where this will, or is likely to, result in the acquisition of legally privileged items. The notification must address the same considerations as described in paragraph 8.40. The senior official, who must not be a member of the public authority to whom the bulk equipment interference warrant is addressed, must in any case where the intention is to acquire items subject to legal privilege, apply the same tests and considerations as described in paragraph 8.41 and 8.42. The authorised person is prohibited from accessing the items until he or she has received approval from the senior official authorising the selection of the items subject to legal privilege.

8.46 In the event that privileged items are inadvertently and unexpectedly selected for examination (and where the enhanced procedure in paragraph 8.40 has consequently not been followed), any item so obtained must be handled strictly in accordance with the provisions of this chapter. No further privileged items may be selected for examination by reference to that factor unless approved by the senior official as set out in paragraph 8.45.

[33] See chapter 6.

[34] Senior official is defined in section 173 of the Act as “senior official” means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty’s Diplomatic Service.

Lawyers' material

8.47 Where a lawyer, acting in this capacity, is the subject of a targeted equipment interference warrant or a targeted examination warrant or whose material has otherwise been selected for examination in accordance with section 179, it is possible that a substantial proportion of the material which will be obtained or examined will be between the lawyer and his or her client(s) and will be subject to legal privilege. Therefore, in any case where the subject of a targeted equipment interference warrant, a targeted examination warrant or whose material has been selected for examination is known to be a lawyer acting in this capacity the application or notification must be made on the basis that it is likely to acquire material subject to legal privilege and the provisions in paragraphs 8.40 - 8.46 will apply, as relevant. This paragraph does not prevent an application being made on the grounds that the lawyer is under investigation for serious criminal offences.

8.48 Any such case should also be notified to the IPC during his or her next inspection and any material which has been retained should be made available to the Commissioner on request.

Handling, retention and deletion

8.49 In addition to safeguards governing the handling and retention of material as provided for in sections 122 and 177 of the Act, officials who analyse material obtained by equipment interference should be alert to any communications or items which may be subject to legal privilege.

8.50 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 122(4). If not, the material should be securely destroyed as soon as possible.

8.51 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 122(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

8.52 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.

8.53 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 legally privileged material, 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 legally privileged material in order to gain a litigation advantage over another party in legal proceedings.

8.54 In order to safeguard against any risk of prejudice or accusation of abuse of process, public authorities must also take all reasonable steps to ensure that lawyers or other officials with conduct of legal proceedings should not see legally privileged material relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the 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

8.55 In those cases where legally privileged material has been obtained via equipment interference, identified as such and then retained, the matter should be reported to the IPC 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.

8.56 For the avoidance of doubt, the guidance in paragraphs 8.40 to 8.55 takes precedence over any contrary content of an agency's internal advice or guidance.

9 Record keeping and error reporting

Records

9.1 Records must be available for inspection by the IPC and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of RIPA), particularly where continuing conduct is alleged. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to five years. The following information relating to all warrants for equipment interference should be centrally retrievable for at least three years:

- all applications made for warrants and for renewals of warrants;
- the date when a warrant is given;
- whether a warrant is approved under urgency procedures;
- where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner;
- the details of what equipment interference has occurred;
- the result of periodic reviews of the warrants;
- the date of every renewal;
- the date when any instruction was given by the Judicial Commissioner to cease the equipment interference; and
- where relevant, the directions issued by the Judicial Commissioner should they refuse to approve an urgent warrant.

9.2 Records should also be kept of the arrangements by which the requirements of sections 122(3) and 177(3) (minimisation of copying and distribution of material) and sections 122(6) and 177(6) (destruction of material) are to be met.

9.3 Records should also be kept by the relevant warrant issuing department. This will include:

- All advice provided to the Secretary of State or law enforcement chief to support their consideration as to whether to issue or renew the equipment interference warrant; and
- Where the issuing of any application is not approved by the Judicial Commissioner, the grounds for refusal as given by the Judicial Commissioner and any associated advice/applications to the IPC if there is an appeal.

9.4 Each relevant equipment interference agency must also keep a record of the information below to assist the IPC in carrying out his or her statutory functions.

9.5 **Targeted warrants:** For the purposes of these record keeping requirements a targeted warrant should be taken as referring to a targeted equipment interference warrant or a targeted examination warrant, issued under part 5 of the Act. In recording this information, each relevant authority must keep a record of:

- The number of applications made by or on behalf of the equipment interference agency for a targeted equipment interference warrant;
- The number of applications for a targeted equipment interference warrant that were refused by an issuing authority;
- The number of decisions to issue a targeted equipment interference warrant that were refused by a Judicial Commissioner;
- The number of occasions that a referral was made by an issuing authority to the IPC, following the decision of a Judicial Commissioner to refuse a targeted equipment interference warrant;
- The number of targeted equipment interference warrants issued by the issuing authority and approved by a Judicial Commissioner;
- The number of targeted equipment interference warrants authorised by the issuing authority and issued by a senior official or appropriate delegate;
- The number of targeted equipment interference warrants authorised by the issuing authority and the number issued by a senior official or appropriate delegate that were subsequently refused by a Judicial Commissioner;
- The number of targeted equipment interference warrants that were renewed by the issuing authority and approved by a Judicial Commissioner;
- The number of targeted equipment interference warrants that the Judicial Commissioner refused to approve the renewal of;
- The number of targeted equipment interference warrants that were cancelled; and
- The number of targeted equipment interference warrants extant at the end of the calendar year.

9.6 For each targeted equipment interference warrant issued by the issuing authority and approved by a Judicial Commissioner (including warrants issued and approved in urgent cases), the relevant agency must also keep a record of the following:

- The statutory purpose(s) specified on the warrant;
- The details of major and minor modifications made to the warrant.

9.7 Bulk warrants:

- The number of applications made for a bulk equipment interference warrant;
- The number of applications for a bulk equipment interference warrant that were refused by a Secretary of State;
- The number of bulk equipment interference warrant that the Judicial Commissioner refused to approve the issuing of;
- The number of occasions that a referral was made by the Secretary of State to the IPC, following the decision of a Judicial Commissioner to refuse the decision to issue a bulk equipment interference warrant;
- The number of bulk equipment interference warrants issued by the Secretary of State and approved by a Judicial Commissioner;
- The number of bulk equipment interference warrants that were renewed by the issuing authority and approved by a Judicial Commissioner;
- The number of bulk equipment interference warrants that were cancelled; and
- The number of bulk equipment interference warrants extant at the end of the year.

9.8 For each bulk equipment interference warrant issued by the Secretary of State and approved by a Judicial Commissioner, the relevant agency must also keep a record of the following:

- The section 165(1)(b) purpose(s) specified on the warrant;
- The number of modifications made to add, vary or remove an operational purpose from the warrant;
- The number of modifications made to add or vary an operational purpose that were made on an urgent basis;
- The number of decisions to issue a modification to add or vary an operational purpose (including on an urgent basis) that the Judicial Commissioner did not approve;
- The number of occasions that a referral was made by the Secretary of State to the IPC, following the decision of a Judicial Commissioner to refuse to modify a bulk equipment interference warrant.

9.9 These records must be sent in written or electronic form to the IPC, as determined by him. Guidance on record keeping will be issued by the IPC. Guidance may also be sought from the Commissioner by equipment interference agencies.

Errors

9.10 This section provides information regarding errors, which are not considered to meet the threshold of a criminal or civil offence.

9.11 A relevant error which must be reported to the IPC is defined in section 209(9) of the Act as an error:

- By a implementing authority or other such persons assisting to give effect to a warrant in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner; and
- Of a description identified for this purpose in a code of practice or in guidance provided by the Commissioner.

9.12 Situations may arise where an equipment interference warrant has been obtained or modified as a result of the relevant agency having been provided with information relating to equipment – for example, by another domestic intelligence agency, police force or CSP – which later proved to be incorrect, due to an error on the part of the person providing the information, but on which the relevant agency acted in good faith. Whilst these actions do not constitute a relevant error on the part of the relevant agency, such occurrences should be brought to the attention of the Commissioner.

9.13 Proper application of the Investigatory Powers Act and thorough procedures for operating its provisions, including for example the careful preparation and checking of warrants, modifications and schedules, should reduce the scope for making errors whether by the implementing authority, CSPs or other persons assisting in giving effect to the warrant.

9.14 Any failure by the implementing authority or such other persons providing assistance to apply correctly the process set out in this code will increase the likelihood of an error occurring.

9.15 All errors described in paragraph 9.11 of this Code must be reported to the Commissioner. Errors can have very significant consequences on an affected individual's rights.

9.16 Reporting of errors will draw attention to those aspects of the equipment interference process that require further improvement to eliminate errors and the risk of undue interference with any individual's rights.

9.17 An error can only occur after equipment interference has commenced. This section of the code cannot provide an exhaustive list of possible errors. Examples could include:

- equipment interference as described in the Act has, or is believed to, have occurred without valid authorisation;
- equipment interference has taken place that would not have occurred but for conduct or an omission of the part of a member of the relevant agency or CSP;
- human error, such as incorrect transposition of equipment information from an application to a warrant or schedule which leads to the wrong material being acquired;
- warranted equipment interference has taken place on a piece of equipment but the material does not in the event relate to the intended subject where information available at the time of seeking a warrant could reasonably have indicated this;
- a material failure to adhere to the arrangements in force under section 122 of the Act relating to material obtained by targeted equipment interference, or the safeguards relating to material obtained by bulk equipment interference contained in sections 177 or 179 of the Act. For example:
  - over-collection caused by software or hardware errors;
  - unauthorised selection/examination of communications; or
  - unauthorised or incorrect disclosure of material;
  - failure to effect the cancellation of equipment interference.

9.18 When an error has been made, the implementing authority or other person which made the error (i.e. the CSP) must report the error to the Investigatory Powers Commissioner as soon as reasonably practicable after it has been established an error has occurred. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full.

9.19 If the implementing authority discovers a CSP error they should inform the Commissioner and the CSP of the error straight away to enable the CSP to investigate the cause of the error and report it themselves.

9.20 The report sent to Commissioner in relation to any error must include details of the error, the cause, the amount of material relating to the error obtained or disclosed, any unintended collateral intrusion, any analysis or action taken, whether the material has been retained or destroyed and, a summary of the steps taken to prevent recurrence. Wherever possible, technical systems should incorporate functionality to minimise errors. A senior person within that organisation must undertake a regular review of errors.

9.21 The Commissioner will keep under review the scope and nature of errors and issue guidance as necessary, including guidance on the format of error reports.

Serious errors

9.22 Section 209 of the Act states that the Commissioner must inform a person of any relevant error relating to that person which the Commissioner considers to be a serious error and that it is in the public interest for the person concerned to be informed of the error.

9.23 In circumstances where a relevant error is deemed to be of a serious nature, the Commissioner may therefore investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

9.24 If the Commissioner concludes that the error has caused significant prejudice or harm to the person concerned, the Commissioner must also decide whether he considers that it is in the public interest for the person concerned to be informed of the error. In making this decision, the Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned; and
- the extent to which disclosing the error would be contrary to the public interest or prejudicial to:
- national security the prevention or detection of serious crime
- the economic well-being of the United Kingdom; or
- the continued discharge of the functions of any of the Security and Intelligence Agencies.

9.25 Before making its decision, the Commissioner must ask the equipment interference agency which has made the error to make submissions on the matters above.

10 Oversight

10.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints against public authority use of certain investigatory powers, including those covered by this code, as well as conduct by or on behalf of any of the intelligence agencies and is the only appropriate tribunal for human rights claims. Any complaints about the use of powers as described in this code should be directed to the IPT.

10.2 The IPC, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The IPC may undertake these inspections, as far as they relate to the IPC's statutory functions, entirely on his or her own initiative or they may be asked to investigate a specific issue by the Prime Minister

10.3 The IPC will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the IPC must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers must, by law, offer all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

10.4 Anyone working for a public authority or communications service provider who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner, who will consider them. In particular, any person who exercises the powers described in the Act or this code must, in accordance with the procedure set out in chapter 9, report to the Commissioner any action undertaken which they believe to be contrary to the provisions of this code. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority. The Commissioner may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the IPT.

10.5 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to an individual who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the individual affected. Further information on errors can be found in chapter 9 of this code. The public body who has committed the error will be able to make representations to the Commissioner before they make their decision on whether it is in the public interest for the individual to be informed. The Commissioner must also inform the affected individual of their right to apply to the Investigatory Powers Tribunal (see Complaints section for more information on how this can be done) who will be able to fully investigate the error and decide if a remedy is appropriate. The Commissioner must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the national interest. Only the Prime Minister will be able to authorise redactions to the Commissioner's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

10.6 The Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publically available subject to public interest considerations. Public authorities and communications service providers may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce guidance for public authorities on how to apply and use Investigatory Powers. Wherever possible this guidance will be published in the interests of public transparency.

10.7 Further information about the IPC, their office and their work may be found at:

11 Complaints

11.1 The IPT has jurisdiction to investigate and determine complaints against public authority use of investigatory powers and human rights claims against the security and intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

11.2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination.

11.3 This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: www.ipt-uk.com. Alternatively information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal

PO Box 33220

London

SWIH 9ZQ

11.4 If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

12 Annex A

Schedule 6: Issue of warrants under section 101 etc.

Part 1

TABLE: PART 1

Law enforcement chiefs	*Appropriate delegates*	*Appropriate law enforcement officers*
The Chief Constable of a police force maintained under section 2 of the Police Act 1996.	The person who is the appropriate deputy chief constable for the purposes of section 12A(1) of the Police Act 1996. The person holding the rank of assistant chief constable designated to act under section 12A(2) of that Act. If it is not reasonably practicable for either of those persons to act, any other person holding the rank of assistant chief constable in the force.	A member of the police force, a member of a collaborative force or a National Crime Agency officer who is included in a collaboration agreement with the police force.
The Commissioner, or an Assistant Commissioner, of the metropolitan police force.	A person holding the rank of commander in the metropolitan police force.	A member of the metropolitan police force, a member of a collaborative force or a National Crime Agency officer who is included in a collaboration agreement with the metropolitan police force.
The Commissioner of Police for the City of London.	The person authorised to act under section 25 of the City of London Police Act 1839 or, if it is not reasonably practicable for that person to act, a person holding the rank of commander in the City of London police force.	A member of the City of London police force, a member of a collaborative force or a National Crime Agency officer who is included in a collaboration agreement with the City of London police force.

The chief constable of the Police Service of Scotland.	Any deputy chief constable or assistant chief constable of the Police Service of Scotland who is designated for the purpose by the chief constable.	A constable of the Police Service of Scotland.
The Chief Constable or a Deputy Chief Constable of the Police Service of Northern Ireland.	A person holding the rank of assistant chief constable in the Police Service of Northern Ireland.	A member of the Police Service of Northern Ireland.
The Director General of the National Crime Agency.	A senior National Crime Agency Officer designated for the purpose by the Director General of the National Crime Agency.	A National Crime Agency officer or a member of a collaborative police force.
The Chief Constable of the British Transport Police.	A person holding the rank of deputy or assistant chief constable in the British Transport Police.	A member of the British Transport Police.
The Chief Constable of the Ministry of Defence Police.	A person holding the rank of deputy chief constable or assistant chief constable in the Ministry of Defence Police.	A member of the Ministry of Defence Police.
The Provost Marshal of the Royal Navy Police.	A person holding the position of deputy Provost Marshal in the Royal Navy Police.	A member of the Royal Navy Police.
The Provost Marshal of the Royal Military Police.	A person holding the position of deputy Provost Marshal in the Royal Military Police.	A member of the Royal Military Police.
The Provost Marshal of the Royal Air Force Police.	A person holding the position of deputy Provost Marshal in the Royal Air Force Police.	A member of the Royal Air Force Police.

TABLE: PART 2

Law enforcement chiefs	*Appropriate delegates*	*Appropriate law enforcement officers*
An immigration officer who is a senior official and who is designated for the purpose by the Secretary of State.	A senior official in the department of the Secretary of State by whom functions relating to immigration are exercisable who is designated for the purpose by the Secretary of State.	An immigration officer.
An officer of Revenue and Customs who is a senior official and who is designated for the purpose by the Commissioners for Her Majesty's Revenue and Customs.	An officer of Revenue and Customs who is a senior official and who is designated for the purpose by the Commissioners for Her Majesty's Revenue and Customs.	An officer of Revenue and Customs.
A designated customs official who is a senior official and who is designated for the purpose by the Secretary of State.	A designated customs official who is a senior official and who is designated for the purpose by the Secretary of State.	A designated customs official.
The Chair of the Competition and Markets Authority.	An officer of the Competition and Markets Authority designated by it for the purpose.	An officer of the Competition and Markets Authority.
The chairman or a deputy chairman, of the Independent Police Complaints Commission.	A member (other than the chair or a deputy chairman) of the Independent Police Complaints Commission who is designated by the chairman for the purpose.	A person designated under paragraph 19(2) of Schedule 3 to the Police Reform Act 2002 to take charge of, or to assist with, the investigation to which the warrant under section 100(1) relates (or would relate if issued)
The Police Investigations and Review Commissioner.	A staff officer of the Police Investigations and Review Commissioner who is designated by the Commissioner for the purpose.	A staff officer of the Police Investigations and Review Commissioner.

Home Office

Communications Data

DRAFT Code of Practice

Autumn 2016

Communications Data

DRAFT Code of Practice

Published for consultation alongside the Investigatory Powers Bill

Autumn 2016

Contents

Section 1

Introduction

1 Introduction

1.1 This code of practice relates to the powers and duties conferred or imposed under Parts 3 and 4 of the Investigatory Powers [Act 2016] ('the Act'). Section 2 of this code provides guidance on the procedures to be followed when acquisition of communications data takes place under the provisions in Part 3 of the Act ('Part 3'). Section 3 of this code provides guidance on the procedures to be followed when communications data is retained under Part 4 of the Act ('Part 4').

1.2 Sections 1, 2 and 4 of this code are relevant to relevant public authorities within the meaning of the Act and to communication service providers ('CSPs')[1]. The relevant public authorities are set out in Schedule 4 of the Act.

1.3 Section 12 of the Act (with Schedule 2) abolishes or amends other information gathering powers in law which provided for access to communications data without appropriate safeguards. Accordingly, relevant public authorities for the purposes of Part 3 should not use other statutory powers to obtain communications data from a postal or telecommunications operator unless:

- That power deals with telecommunications operators,postal operators, or a class of such operators;
- That power can be used in connection with the regulation of telecommunications operators, services or systems; or such postal operators or services;[2]
- That power can be used to acquire communications data relating to postal items crossing the United Kingdom border; or
- That power is authorised by a warrant or order issued by the Secretary of State or a person holding judicial office.

1.4 Such powers should only be used to obtain communications data from a CSP where it is not possible for the public authority to obtain the data under the Act[3].

1.5 Relevant public authorities should also not require, or invite, any postal or telecommunications operator to disclose communications data by relying on any exemption to the principle of non-disclosure of personal data set out under Part 4 of the Data Protection Act 1998 ('the DPA').

1.6 Sections 1, 3 and 4 of this code are relevant to CSPs who have been issued with a data retention notice under Part 4.

---

1 See paragraph 2.1 for a definition of communications service provider.

2 The Office of Communications or a statutory co-regulator it approves may, for example, use powers conferred by or under Part 2 of the Communications Act 2003 to obtain communications data from a telecommunications operator for the purpose of carrying out the regulatory functions given to them under that Part of that Act.

3 Section 12(3) provides that regulatory powers and powers which can acquire postal data in relation to items crossing the border may only be exercised by the public authority if it is not possible for the public authority to use a power under the Act to secure the disclosure of the data.

1.7 This code should be readily available to members of a relevant public authority involved in the acquisition of communications data under the Act, and to CSPs involved in the retention of communications data and/or its disclosure to public authorities under the Act.

1.8 The Act provides that persons exercising any functions to which this code relates must have regard to the code. Although failure to comply with the code does not, of itself, make a person liable to criminal or civil proceedings.

1.9 The Act provides that the code is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to a question before any court or tribunal hearing any such proceedings, or to the Investigatory Powers Tribunal (IPT) or to the Investigatory Powers Commissioner (the 'IPC') or the Information Commissioner when overseeing the powers conferred by the Act, it may be taken into account.

1.10 The Interception of Communications Code of Practice, Bulk Acquisition Code of Practice and Equipment Interference Code of Practice provide guidance on procedures to be followed in relation to those Parts of the Act.

1.11 The exercise of powers and duties under Parts 3 and 4 of the Act and this code are kept under review by the Investigatory Powers Commissioner ('the Commissioner') appointed under section 205 of the Act and by his Judicial Commissioners and inspectors who work from the Investigatory Powers Commission. Duties under Part 4 of the Act and this code in relation to the security, integrity and destruction of data retained under a notice are subject to audit by the Information Commissioner. CSPs must comply with reasonable requests from the Information Commissioner in relation to his audit role.

1.12 The Home Office may issue further advice directly to public authorities and CSPs as necessary.

1.13 This code extends to the United Kingdom[4].

1.14 For the avoidance of doubt, the guidance in this code takes precedence over any contrary content of a public authority's internal advice or guidance.

[4] This code and the provisions in Parts 3 and 4 of the Act do not extend to the Crown Dependencies and British Overseas Territories. Note that chapter 11 includes sections on acquisition of communication data on behalf of overseas authorities and the transfer of communications data to overseas authorities.

2 Scope and definitions

Communications service provider

2.1 The obligations under Parts 3 and 4 of the Act apply to telecommunications operators and postal operators. Throughout this code, communications service provider ('CSP') is used to refer to a telecommunications operator or postal operator. CSP is not a term used in the Act.

2.2 A telecommunications operator is a person who offers or provides a telecommunication service to persons in the UK or who controls or provides a telecommunication system which is, (in whole or in part) in or controlled from the UK. A postal operator is a person providing a postal service to a person in the UK. These definitions make clear that obligations in the Parts of this Act to which this code apply cannot be imposed on communication service providers whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK.

2.3 Section 237 of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the telecommunication service provider); and defines 'telecommunications system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. The definition of 'telecommunications service' in the Act is intentionally broad so that it remains relevant for new technologies.

2.4 The Act makes clear that any service which consists in, or includes, facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunications system is included within the meaning of 'telecommunications service'. Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.

2.5 The definition of a telecommunications operator also includes application and website providers but only insofar as they provide a telecommunication service. For example an online market place may be a telecommunications operator as it provides a connection to an application/website. It may also be a telecommunications operator if and in so far as it provides a messaging service.

2.6 Telecommunications operators may also include those persons who provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in commercial premises such as hotels or public premises such as airport lounges or public transport.

2.7 In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider, or where there are security implications in doing so, the data may be sought from the CSP which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of communications data for example, where a hotel is in possession of data identifying specific telephone calls originating238 of the Act defines 'postal service' to mean any service which consists in one or more of the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items and which is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to transmit postal items from place to place.

2.8 For the purposes of the Act a postal item includes letters, postcards and their equivalents as well as packets and parcels. It does not include freight items such as containers. A service which solely carries freight is not considered to be a postal service under the Act. Where a service carries both freight and postal items it is only considered to be a postal service in respect of the transmission of postal items.

Composition of communications

2.9 For the purposes of the Act communications may comprise two broad categories of data: systems data and content. Some communications may consist entirely of systems data. Section 237(6)(b) makes clear that anything which is systems data is, by definition, not content. When permitted by the Act, certain data may also be separated from the remainder of a communication in circumstances where, if it were so separated, it would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication. This is identifying data. Systems data and identifying data may be obtained by interception or equipment interference warrants under Parts 2 and 5, and 6 of the Act. Further details on systems and identifying data can be found in the interception and equipment interference codes of practice.

2.10 Communications data is a subset of systems data. Section 237(5) is clear that, even though systems data cannot be content, communications data is limited to data which does not reveal anything of what might reasonably be considered to be the meaning of the communication, excepting any meaning arising from the fact of the communication or transmission of the communication. That is, any systems data which would, in the absence of section 237(6)(b), be content, cannot be communications data.

2.11 Any communications data obtained as part of systems data under an interception warrant is intercept material. Any such data must be treated in accordance with the restrictions on the use of intercept material in the Interception Code of Practice. Communications data obtained as part of systems data under an equipment interference warrant must be handled in accordance with the safeguards set out in the Equipment Interference Code of Practice.

Communications data

2.12 The term 'communications data' includes the 'who', 'when', 'where', and 'how' of a communication but not the content i.e. what was said or written[5].

2.13 It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning[6], of the communication.

2.14 It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

2.15 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services – i.e. postal services or telecommunications services.

Telecommunications definitions

2.16 Communications data in relation to telecommunications operators' services and systems includes data held or obtainable by a CSP or which is available directly from a telecommunications system and which:

- Is about an entity to which a telecommunication service is provided **and** relates to the provision of the service;
- Is comprised in, included as part of, attached to or logically associated with a communication for the purposes of a telecommunication system that facilitates the transmission of that communication; or
- Relates to the use of a service or system; or
- Is about the architecture of a telecommunication system.

2.17 The first limb of the definition includes information about any person to whom a service is provided, whether a subscriber or guest user and whether or not they have ever used that service. For example this may include information about the person associated with an email address even if that email address has not been used since its creation.

2.18 An entity (see below for further details) can also include devices so this limb would cover information about the devices owned by a customer as well as the services to which the owner of the devices subscribes. This data may include names and addresses of subscribers.

---

5 See paragraph 2.45 for the definition of content.

6 As set out at section 237(6)(a)

2.19 Importantly this limb is limited to data held or obtained by the CSP in relation to the provision of a telecommunications service – it does not include data which may be held about a customer by a CSP more generally which are not related to the provision of a telecommunications service. For example for a social media provider data such as the status of the account, contact details for the customer and the date a person registered with the service would all be communications data as they relate to the use of the service. However, other data held by the provider about a customer which does not relate to the provision of the telecommunication service, including personal information such as political or religious interests included in profile information, is not within scope of the definition of communications data.

2.20 The second limb includes any information that is necessary to get a communication from its source to its destination, such as dialled telephone number or Internet Protocol (IP) address. It includes data which:

- Identifies the sender or recipient of a communication or their location;
- Identifies or selects the apparatus used to transmit the communication;
- Comprises signals which activate the apparatus used (or which is to be used to) to transmit the communication; and
- Identifies data as being part of a communication.

2.21 Communications data under this limb also includes data held or capable of being obtained, by the CSP which is logically associated with a communication for the purposes of the telecommunications system by which the communication is being, or may be, transmitted. This might include, for example domain name service (DNS) requests which allow communications to be routed across the network. It also includes data that facilitates the transmission of future communications (regardless of whether those communications are, in fact, transmitted).

2.22 Only information falling within this second limb can be obtained directly from a telecommunications system by a public authority.

2.23 The third limb covers other information held by a CSP about the use of the service such as billing information.

2.24 The fourth limb additionally includes data held by a CSP about the architecture of the telecommunications system (sometimes referred to as ‘reference data’). This may include the location of cell masts or Wi-Fi hotspots. This information itself does not contain any information relating to specific persons and its acquisition in its own right does not interfere with the privacy of any customers. However, this data is often necessary for the public authority to interpret the data received in relation to specific communications or users of a service.

2.25 All communications data held by a telecommunication operator or obtainable from a telecommunications system falls into two categories:

- Entity data – This data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).
- Events data – Events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

2.26 The authorisation levels required to access communications data reflect the fact that the set of events data as a whole contains the more intrusive communications data, including information on who has been in communication with whom, a person's location when their mobile device connects to the network and internet connection records. The authorisation levels in Schedule 4 to the Act reflect the differing levels of intrusiveness of the data. For example the police can authorise access to entity data at Inspector level but events data is authorised at Superintendent level.

2.27 There are some circumstances where a CSP will need to process events data in order to respond to a request for entity data. In such circumstances it is the type of data that is disclosed which determines the authorisation level required e.g. if a public authority wants to know the identity of a person using an IP address at a specific time and date then the CSP can provide this response as entity data even though it may have to obtain this information from event data relating to a specific communication.

2.28 Where a public authority provides events data to a CSP as part of a request for entity data then the CSP may include that events data in the response to the entity data request. Taking the example above the CSP could include the time and date of the communication as part of the response without the need for it to be authorised as an event.

Entity data

2.29 Entity data covers information about a person or thing, and about links between a telecommunications service, part of a telecommunication system and a person or thing, that identify or describe the person or thing. This means that individual communication devices such as phones, tablets and computers are entities. The links between a person and their phone are therefore entity data but the fact of or information about communications between devices on a network at a specific time and for a specified duration would be events data.

2.30 Examples of entity data include:

- 'Subscriber checks' such as "who is the subscriber of phone number 01632 960 224?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- Subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- Information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- Information about apparatus/ devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes[7]; and

[7] This includes PUK (Personal Unlocking Key) codes for mobile phones. These are initially set by the handset manufacturer and are required to be disclosed in circumstances where a locked handset has been lawfully seized as evidence in criminal investigations or proceedings.

- Information about selection of preferential numbers or discount calls.

2.31 Entity data can change over time. So, for example if a person moves house the address held by a CSP will change. The fact of that is an attribute of the entity (the person) and not a communication event.

2.32 Some CSPs may retain user passwords[8] where already available in the clear for business purposes. In this context passwords would constitute entity data. Any information, such as a password, giving access to the content of any stored communications or access to the use of a communication service may only be sought from a CSP in the following circumstances:

- Where such information is necessary in the interests of national security; or
- For preventing death, injury or damage to health.

2.33 Passwords cannot be used by a public authority to access the content of stored communications or any communication service without appropriate lawful authority, for example the consent of the person, an equipment interference warrant, an interception warrant, property interference authorisation or directed surveillance authorisation.

Events

2.34 Events data covers information about events taking place across a telecommunications system at a specific time and for a specified duration. Communications data is limited to communication events describing the transmission of information between two or more entities over a telecommunication service. This will include information which identifies, or appears to identify, any person, apparatus[9] or location to or from which a communication is transmitted. It does not include non-communication events such as a change in address or telephone number for a customer.

2.35 Examples of events data include, but are not limited to:

- Information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- Information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- Information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- Routing information identifying apparatus through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);

---

[8] In many cases a CSP will actually retain a password hash rather than the password itself. This is an encrypted form of the password. When you enter the password to use a service it is encrypted using the same method and the password hash generated is checked against the hash held by a CSP meaning the CSP never needs to retain the actual passwords. A hash is unlikely to be of any use to a public authority and where that is the case it is unlikely to be sought.

[9] 'Apparatus' is defined in section 239 of the Act to mean 'any equipment, machinery, device (whether physical or logical) and any wire or cable'.

- Itemised telephone call records (numbers called)[10];
- Itemised records of connections to internet services;
- Itemised timing and duration of service usage (calls and/or connections);
- Information about amounts of data downloaded and/or uploaded;
- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

Postal definitions

2.36 Communications data in relation to a postal service is defined at section 238(3) of the Act and includes:

- Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted;
- Data relating to the use made by a person of a postal service;
- Information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service **and** which relates to the provision of the service.

2.37 The data in the first limb includes any information that identifies, or appears to identify, any person or location to or from which a communication is or may be transmitted and includes:

- Anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item's postal routing, sender or recipient;
- Records of correspondence checks comprising details of data from postal items in transmission to a specific address; and
- Online tracking of communications (including postal items and parcels).

2.38 The second limb includes data relating to the use made by any person of a postal service, or any part of it includes:

- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including redirection services;
- The price paid to send an item and the postage class used;
- Records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

2.39 The third limb of the definition includes information about any person to whom a service is provided, whether a subscriber or guest user and whether or not they have ever then used that service. For example this may include information about the person associated with a PO Box even if that PO Box address has never received any mail.

[10] Itemised bills can include an indication of the cost for receiving communications, for example calls and messages received by a mobile telephone that has been 'roaming' on another network.

2.40 As with the telecommunications definitions this limb does not include data which may be held about a customer by a CSP more generally which are not related to the provision of a postal service.

2.41 Examples of data within the third limb include:

- Information about the subscriber to a PO Box number or a postage paid impression used on bulk mailings;
- Information about the provision to a subscriber or account holder of forwarding/redirection services, including delivery and forwarding addresses;
- Subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments.

2.42 Postal data is defined in section 238(4) of the Act and includes specified categories of data written on the outside of a postal item. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is postal data.

2.43 Those public authorities which are able to authorise access to entity data at a lower level of seniority may also authorise access to the third limb of postal communications data at 238(3)(c) of the Act at the same level.

Content

Telecommunications definitions

2.44 The content of a communication is defined in section 237(6) of the Act as the data which reveals anything of what might be reasonably be considered to be the meaning (if any) of that communication.

2.45 When one person sends a message to another what they say or what they type in the subject line or body of an email is the content. However there are many ways to communicate and the definition covers the whole range of telecommunications. What is consistent is that the content will always be the part of the communication (whether it be the speech of a phone call or the text of an email) that conveys the substance or meaning the sender is intending to convey to the recipient. It is that meaning that the Act defines as content.

2.46 When a communication is sent over the telecommunication systems it can be carried by multiple providers. Each provider may need a different set of data in order to route the communication to its eventual destination. Where data attached to a communication is identified as communications data it continues to be communications data, even if certain providers have no reason to look at this data (see third party data below). The definition of content ensures that the elements of a communication which are considered to be content do not change depending on which communication provider is carrying the communication.

2.47 There are two exceptions to the definition of content (set out in section 237(6)). The first addresses inferred meaning. When a communication is sent, the simple fact of the communication conveys some meaning, e.g. it can provide a link between persons or between a person and a service. This exception makes clear that any communications data associated with the communication remains communications data and the fact that some meaning can be inferred from it does not make it content.

2.48 The second makes clear that systems data cannot be content[11].

Postal definitions

2.49 In the postal context anything included inside a postal item, which is in transmission, will be content. Any message written on the outside of a postal item, which is in transmission, may be content and fall within the scope of the provisions for interception of communications. For example, a message written by the sender for the recipient will be content but a message written by a postal worker concerning the delivery of the postal item will not.

Web browsing and communications data

2.50 Browser software provides one way for users to access web content (although there are other commonly used mechanisms, such as dedicated applications). When using a browser to access the web, a user may enter a web address. These are also referred to as URLs (uniform resource locators).

2.51 The URL is normally converted from a human understandable form to numeric IP addresses by means of DNS in order to transmit information over the internet.

2.52 URLs follow a standardised structure and will always contain:

- The scheme - web data is commonly transferred by the http protocol.
- The host identifier, which can be a fully or partially qualified domain name. A web communication requires the fully qualified domain name (FQDN) in order for the process to be completed. Use of a partially qualified domain name (PQDN) will either end up with a FQDN being generated for the browser, or a failed communication. Some web sites split their content across a number of servers which may be identified by FQDNs, for example news.newssite.co.uk or bbc.co.uk. Because the content is split across a number of servers the fully qualified domain name routes the communication to the correct server.

2.53 These elements of a URL are necessary to route a communication to the intended recipient and are therefore communications data. Although fully qualified domain names provide an indication of the type of content that the server being accessed contains they do not identify individual items of content and therefore the exception to the definition regarding inferred meaning ensures that such elements of the URL are not considered content.

2.54 Additionally URLs may, but do not always, contain:

[11] See interception and equipment interference codes of practice for more information

- The port, which is an extended part of the IP address, and is required to make the communication process function.
- The userinfo, which does not have to appear. It covers usernames and authorisations.
- The path and optional parameters, which are analogous to a file path on a computer. In the example of socialmedia.com/profile/home the /profile/home is the path.
- The optional query parameters and fragments. These query parameters (identified by a '?' in the URL) contain data that doesn't fit within a hierarchical path structure and can locate certain content.

2.55 With the exception of the port, and in certain circumstances the userinfo, these elements of a URL, where present, will not constitute communications data.

2.56 An authorisation under Part 3 of the Act or retention notice under Part 4 of the Act may only authorise the acquisition or retention of those elements of a URL which constitute communications data.

Relevant communications data

2.57 A data retention notice under the Act may only require the retention of relevant communications data. Relevant communications data is defined in section 84 of the Act and is a subset of communications data.

2.58 It is data which may be used to identify or assist in identifying any of the following:

- The sender or recipient of a communication (whether or not a person) – this can include phone numbers, email addresses, user identities and other information which can identify a customer such as names, addresses, account details and other contact information. In the context of internet access this can include source and destination IP addresses, port numbers and the relevant elements of URLs[12];
- The time or duration of a communication – this can include the time and duration of phone calls, the time of emails, connections on the internet or internet access sessions;
- The type, method or pattern, or fact, of communication – this can include billing records or other records showing the usage of a communication system;
- The telecommunications system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted – this can include the identities of cell masts or Wi-Fi access points to which a device has connected; or
- The location of any such system – this can include the physical location of phones or other communication devices or the location of cell masts or Wi-Fi access points to which they connect. The data that can be retained under a notice includes the data which would form an internet connection record (see below).

[12] See section on web browsing and communications data, paragraphs 2.50-2.56.

2.59 The data to be retained under a retention notice will be set out in the notice. A notice may provide for the retention of data that is necessary to enable the CSP to correlate the above data and transmit it in response to requests. This may include, but is not limited to, customer reference numbers.

2.60 A data retention notice can never require a CSP to retain the content of communications or third party data (see paragraph 2.68).

Internet connection record

2.61 An Internet connection record ('ICR') is a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet. An ICR is communications data which may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunications system for the purpose of obtaining access to, or running, a computer file or program. It comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication. In most cases ICRs will be held by internet access providers which are telecommunications operators which provide access to the internet and can include a home broadband connection, mobile internet or publicly available Wi-Fi.

2.62 An ICR will only identify the service that a customer has been using. It is not intended to show what a customer has been doing on that service. For example many social media apps on a device maintain persistent connections to a service. Even in this case the relevant ICR will signpost the service accessed by the device, enabling the public authority to make further enquiries of the service provider identified through an ICR. An ICR may consist of:

- A customer account reference – this may be an account number or an identifier of the customer's device or internet connection;
- The date/time of the start and end of the event or its duration;
- The source IP address and port;
- The destination IP address and port – this is the address of the service accessed on the internet and could be considered as equivalent to a dialled telephone number. The port additionally provides an indication of the type of service (for example website, email server, file sharing service, etc.);
- The volume of data transferred in either, or both, directions;
- The name of the internet service or server connected to; and
- Those elements of a URL which constitute communications data – this is the web address which is the text you type in the address bar in an internet browser. In most cases this will simply be the domain name – e.g. socialmedia.com.

2.63 The core information that is likely to be included is: an account reference, a source IP and port address, a destination IP and port address and a time/date. However,

there is no single set of data that constitutes an internet connection record, it will depend on the service and service provider concerned.

2.64 Where a data retention notice is issued requiring a CSP to retain ICR the specific data that an internet access provider may be required to retain will be discussed with the provider before the requirement is imposed[13].

2.65 A CSP cannot be required to retain third party data as part of an ICR.

2.66 ICRs can include connections which are made automatically by a person's browser or device.

Third party data

2.67 Where a communication is sent there may be multiple providers involved in the delivery of the communication. Each provider may require different elements of communications data to route the communication. For example, when sending an email there will be the email provider, the internet access provider for the sender and the internet access provider for the recipient. The email provider will require the email address to route the communication but neither internet access provider has any need to see or access the full email address in order to connect the sender or recipient to the mail server.

2.68 Where one CSP is able to see the communications data in relation to applications or services running over their network, in the clear, but does not process that communications data in any way to route the communication across the network this is regarded as third party data. A CSP is considered to process data to route a communication if it specifically looks at an item of data in order to determine what action to take or if it has a set of rules in place which determine how a communication should be routed depending on certain items of data.

2.69 If a CSP has no need to process data to route a communication but extracts and retains this data or a product generated from this data for their own business purposes, such as for network diagnostics, then this is no longer regarded as third party data. This data could be covered by a data retention notice and is available to be acquired under Part 3 of the Act.

2.70 A retention notice **cannot** require a CSP to retain third party data. Accordingly an ICR retained by a CSP may only include data that the CSP itself needs to transmit the communication, unless the CSP retains additional relevant data about the third party service for their own business purposes.

2.71 A communications data authorisation can permit the acquisition by a public authority of third party data on a forward looking basis where necessary and proportionate in relation to a specific investigation. A CSP in receipt of a request or requirement to obtain and disclose third party data need only provide the data where reasonably practicable to do so. A CSP in receipt of a requirement to obtain and disclose third party data which is encrypted by the third party is under no obligation to decrypt such information.

[13] See paragraph 4.67 on issuing notices.

Guidance on definitions

2.72 Where an applicant is unsure of the category of data they are seeking (entity or events data) or what additional communications data may be retained by a CSP for their own business use, the applicant should discuss this with their Single Point of Contact (SPoC). If a SPoC or designated senior officer wish to find out more, they should consult the relevant CSP or contact the Communications Data Knowledge and Engagement Team, currently part of the College of Policing.

2.73 The Home Office may, from time to time, issue further guidance to CSPs or public authorities, on how the definitions in the Act apply.

Part 2

Communications Data Acquisition and Disclosure

3 General extent of powers

Scope of powers, necessity and proportionality

3.1 The acquisition of communications data under Part 3 of the Act will be a justifiable interference with an individual's human rights under Articles 8 and, in certain circumstances, 10 of the European Convention on Human Rights only if the conduct being authorised or required to take place is necessary for the purposes of a specific investigation or operation, proportionate and in accordance with law.

3.2 The Act stipulates that conduct to be authorised or required must be necessary for one or more of the purposes set out in section 58(7) of the Act:

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder; or
- In the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- In the interests of public safety - this purpose should be used by public authorities with functions to investigate specific and often specialised offences or conduct such as accident investigation or for example, a large scale event that may cause injury to members of the public. Public safety should not be interpreted as for purposes relating to crime that impacts on the public, such as the sale of illegal drugs;
- For the purpose of protecting public health – this should be used by public authorities with functions to investigate specific and often specialised offences or conduct such as breaches of health and safety legislation and criminal offences which may risk public health, for example, the supply of controlled medicines without licence or prescriptions;
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- For the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health – this can include those situations where, for example, there is serious concern for the welfare of a vulnerable person including children at imminent risk of being abused or otherwise harmed. It may also include circumstances where a person is missing and the acquiring authority considers there to be a real threat to that person's life or health;
- To assist investigations into alleged miscarriages of justice;
- Where a person ("P") has died or is unable to identify themselves because of a physical or mental condition to assist in identifying P, or to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition; and
- For the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.

3.3 The purposes for which public authorities may seek to acquire communications data are set out in Schedule 4 to the Act (and for local authorities in section 70). The designated senior officer may only consider necessity on grounds open to their public authority and only in relation to matters that are the statutory or administrative function of their respective public authority. The purposes noted above should only be used by a public authority in relation to the specific (and often specialist) offences or conduct that it has been given the statutory function to investigate.

3.4 As set out in section 58(8), the fact that the information that would be obtained under an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the authorisation is necessary on the grounds on which authorisations may be issued. Public authorities are permitted to apply for an authorisation against members or officials of a trade union where that is necessary for one of the stautory purposes listed above and proportionate to what is sought to be achieved.

3.5 There are further restrictions upon the acquisition of ICRs (see chapter 7). ICRs cannot be acquired by local authorities in any circumstances.

3.6 When a public authority wishes to acquire communications data, the designated senior officer must believe that the acquisition, in the form of an authorisation, is necessary. He or she must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

3.7 As well as consideration of the rights of the individual under investigation, consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. An application for the acquisition of communications data should draw attention to any circumstances which give rise to significant collateral intrusion. In such cases it may be appropriate to utilise the filtering arrangements (see chapter 9).

3.8 Particular consideration must also be given, when pertinent, to the right to freedom of expression and the need to protect the public interest in the confidentiality of sources of journalistic information through judicial approval of relevant applications[14].

3.9 Taking all these considerations into account in a particular case, an interference with the rights of an individual may still not be justified because the adverse impact on the rights of another individual or group of individuals is too severe.

3.10 Any conduct where the interference is excessive in relation to the aims of the investigation or operation, or is in any way arbitrary, will not be proportionate.

[14] See section on applications to determine the source of journalistic information beginning at paragraph 6.5 for further information and guidance.

3.11 Before public authorities can acquire communications data, authorisation must be given by the designated senior officer in the relevant authority. A designated senior officer is someone holding a prescribed office, rank or position (or a more senior position), specified in relation to the relevant authority that has been designated for the purpose of acquiring communications data by section 67 of or Schedule 4 to the Act .

3.12 Section 2 of the Act requires a public authority to have regard to the following when granting an authorisation to obtain communications data:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means,
- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.

3.13 The relevant public authorities are set out in Schedule 4 to the Act.

Further guidance on necessity and proportionality

3.14 Training regarding necessity and proportionality should be made available to all those who participate in the acquisition and disclosure of communications data.

Necessity

3.15 In order to justify that an application is necessary, the application needs as a minimum to cover three main points:

- The event under investigation, such as a crime or vulnerable missing person;
- The person, whose data is sought, such as a suspect, witness or missing person, and how they are linked to the event; and
- The communications data, such as a telephone number or IP address, and how this data is related to the person and the event.

3.16 Necessity should be a short explanation of the event, the person and the communications data and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

Proportionality

3.17 Applications should include an outline of how obtaining the data will benefit the investigation or operation. The relevance of the data being sought should be explained and any considerations which might undermine the application.

3.18 This should include explaining how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example the subscriber details of a phone number may be obtainable from a phone book or other publically available sources.

3.19 The relevance of time periods requested must be explained, outlining how these periods are proportionate to the event under investigation.

3.20 An examination of the proportionality of the application should particularly include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

3.21 Collateral intrusion is the obtaining of any information relating to individuals other than the subject(s) of the investigation. The degree of collateral intrusion forms part of the proportionality considerations, and becomes increasingly relevant when applying for events data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion. When there are no meaningful collateral intrusion risks, such as when applying for entity data in relation to a person under investigation, the absence of collateral intrusion should be noted.

3.22 An examination of the proportionality of the application should also involve a consideration of possible unintended consequences and, when relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application.

3.23 Unintended consequences are more likely in more complicated requests for events data or in applications for the data of those in professions with duties of confidentiality. For example, if a journalist is a victim of crime, applications for events data related to that journalist's phone number as part of the criminal investigation may also return some phone numbers of that journalist's sources, with unintended impact on freedom of expression. Such an application may still be necessary and proportionate but the risk of unintended consequences should be considered. The special considerations that arise in such cases are discussed further in the sections on "Communications data involving certain professions" and "Applications to determine the source of journalistic information".

4 General rules on the granting of authorisations

4.1 Acquisition of communications data under the Act involves four roles within a relevant public authority:

- The applicant;
- The designated senior officer;
- The single point of contact; and
- The senior responsible officer.

4.2 The Act provides for acquisition of communications data, by way of an authorisation under section 58. An authorisation granted to a member of a public authority permits that person to engage in conduct which is for the purpose of obtaining data from any person and relates to a telecommunication system or postal service, or data derived from such a system or service. Such conduct may include requiring by notice a postal or telecommunications operator to disclose the relevant communications data held by it, or to obtain and disclose the data whether or not in existence at the time of the authorisation, when it is reasonably practicable for them to do so, in accordance with the authorisation. Authorisations are explained in more detail within this chapter.

4.3 All authorisations and notices must be granted or cancelled in writing or, if not, in a manner that produces a record within the public authority of it having been granted.

4.4 An authorisation may relate to conduct outside the UK and persons outside the UK. Anyone providing a public postal service or a telecommunications service, or who has control of a telecommunication system in the UK, is under a duty to comply with any requirements imposed by notice given to them in pursuance of an authorisation. This applies to any company offering services to customers in the UK, irrespective of where the company is based.

4.5 An authorisation under section 58 of the Act may not be used to acquire communications data directly from a telecommunications network where equipment is interfered with in the process of acquiring communications data. Such activity includes interference with a user device or the network over which the communication is being carried. Such practices may only take place under an equipment interference warrant – see the equipment interference code of practice.

4.6 An authorisation under section 58 of the Act may not be used where it is not possible to determine whether the data being acquired would constitute communications data. Where there is doubt as to whether data other than communications data would be acquired an interception warrant, or where appropriate equipment interference warrant, should be sought.

The applicant

4.7 The applicant is a person involved in conducting an investigation or operation for a relevant public authority who makes an application in writing or electronically for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the designated senior officer, the necessity and proportionality of a specific requirement for acquiring communications data.

4.8 An application may be made orally in exceptional circumstances, but a record of that application must be made in writing or electronically as soon as possible, and certainly within one working day (paragraphs 4.77 - 4.83 provide more detail on urgent procedures).

4.9 An application[15] must:

- Include the name (or designation where relevant for applicants in the Security and Intelligence Agencies (SIA)) and the office, rank or position held by the person making the application;
- Include a unique reference number;
- Include the operation name (if applicable) to which the application relates;
- Specify the purpose for which the data is required, by reference to a statutory purpose under section 58(7) of the Act;
- Describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- Describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- Explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it[16];
- Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- Consider and, where appropriate, describe any possible unintended consequences of the application;
- Where data is being sought from a CSP, specify whether the CSP may inform the subject(s) of the fact that an application has been made for their data; and
- Identify and explain the time scale within which the data is required.

4.10 The application should record subsequently whether it was approved by a designated senior officer, by whom and when that decision was made. If approved, the application form should, to the extent necessary, be cross-referenced to any authorisation granted. The original or a copy of the application must be retained by the SPoC.

---

[15] Public authorities should ensure their application processes are efficient and do not impose unnecessary bureaucracy on their operational staff which goes beyond the requirements of the Act and this code.

[16] See sub-section on further guidance on necessity and proportionality, beginning at paragraph 3.14. This also applies to the next two bullets on collateral intrusion and unintended consequences.

The designated senior officer

4.11 The designated senior officer is a person holding a prescribed office in a relevant public authority[17]. If the designated senior officer believes the acquisition of communications data is necessary and proportionate in the specific circumstances, an authorisation is granted. If the designated person does not consider the case for obtaining the data has been met the application should be rejected and referred back to the SPoC and the applicant.

4.12 It is the designated senior officer's responsibility to consider the application and record their considerations at the time (or as soon as is reasonably practicable) in writing or electronically. They must be able to show that they have understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny. Comments should be tailored to a specific application as this best demonstrates the application has been properly considered.

4.13 If the designated senior officer having read the application considers the applicant has met all the requirements then he or she should simply record that fact. In such cases a simple note should be recorded. There may be circumstances where the designated senior officer having read the case set out by the applicant and the considerations of the SPoC will want to comment why it is still necessary and proportionate to obtain the data despite excessive data being acquired.

4.14 Individuals who undertake the role of designated senior officer must have current working knowledge of human rights principles and legislation, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data under Part 3 of the Act and this code.

4.15 The existence of a defined cadre of designated senior officers within any given organisation will assist the senior responsible officer and SPoC in managing training and compliance requirements. A 'defined cadre' ensures that authorisation may not be given by anyone at the correct grade but by a listed subset of people or roles at that grade who have the appropriate expertise.

4.16 When considering proportionality, the designated senior officer should apply particular consideration to unintended consequences. The seniority, experience and training of the designated senior officer provides them with a particular opportunity to consider possible unintended consequences. Specific additional proportionality issues relating to use of filtering arrangements are detailed at paragraph 9.8.

4.17 Designated senior officers must ensure that they grant authorisations only for purposes and only in respect of types of communications data that a designated senior officer of their office, rank or position in the relevant public authority may grant or give.

[17] See section 61 and Schedule 4 to the Act.

4.18 Where an investigation relates to an allegation of criminal conduct by a member of a public authority, that public authority (or another public authority appointed to investigate the complaint) may use their powers under Part 3 to obtain communications data for the purpose of preventing or detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain communications data under the Act.

4.19 The designated senior officer shall assess the necessity of any conduct to acquire or obtain communications data taking account of any advice provided by the SPoC.

4.20 Designated senior officers must ordinarily be independent from operations and investigations when granting authorisations related to those operations. In practice this means that a designated senior officer should be far enough removed from the applicant's line management chain or the investigation so as to not be influenced by operational imperatives, such as pressure to expedite results on a particular operation. Normally this will mean that the designated senior officer is not within the same department or unit or an integral part of the investigation. It is not considered good practice for applicants to be able to choose a designated senior officer on a case-by-case basis.

4.21 In exceptional circumstances a public authority may not be able to call upon the services of a designated senior officer who is independent from the investigation or operation. This may include cases where delays in locating an independent designated senior officer may pose an immediate threat to life. Such cases would normally be expected to invoke the urgent oral process.

4.22 Three further exceptions to this rule exist. In these cases the senior responsible officer must inform the Commissioner, in advance, of those designated senior officers who would not be independent in such cases. These exceptions are:

- Specialist criminal investigation departments within public authorities which are not law enforcement or intelligence agencies whose small size precludes use of an independent designated senior officer[18];
- Where the investigation or operation concerned is one where there is an exceptional need, in the interests of national security, to keep knowledge of it to a minimum: and
- Where there is an opportunity to obtain information where the opportunity is rare, the time to act is short, and the need to obtain the information is significant and in the interests of national security.

[18] Small public authorities should consider entering into a collaboration agreement under section 75 of the Act.

4.23 In all circumstances where public authorities use designated senior officers who are not independent from an operation or investigation, the senior responsible officer must notify the Commissioner of circumstances and reasons (noting which designated senior officer granted the authorisation) at the next inspection or as otherwise required by the Commissioner. The details of the public authorities and the reasons such measures are being undertaken may be published and included in the Commissioner's report.

4.24 Where a designated senior officer is not independent from the investigation or operation their involvement and their justification for undertaking the role of the designated senior officer must be explicit in their recorded considerations.

4.25 Particular care must be taken by designated senior officers when considering any application to obtain communications data to identify apparatus (such as a mobile telephone) at or within a location or locations and at or between times on a given date or dates where the identity of the apparatus is unknown[19]. Unless the application is based on information that the apparatus was used or was likely to have been used in a particular location or locations at a particular time or times it will, in practice, be rare that any conduct to obtain communications data will be proportionate or the collateral intrusion justified.

4.26 In situations where there is an immediate threat to life (for example a person threatening to take their own or someone else's life or where threats are made to a victim in a kidnap) some CSPs will undertake to adapt their systems beyond the requirements of their normal business practice to be able to assist the relevant public authority in preserving life. The use of such bespoke systems must be proportionate, and any collateral intrusion justified, to the specific circumstances of any investigation or operation.

4.27 Where there is no immediate threat to life in an investigation or operation, any conduct to obtain communications data using any other bespoke systems (for example, those used to trace malicious and nuisance communications) must be reliant upon both the co-operation and technical capability of the CSP to provide such assistance outside of its normal business practice.

The single point of contact

4.28 Before granting an authorisation a designated senior officer must, except in exceptional circumstances (see paragraphs 4.42 – 4.47), have the benefit of the advice of a SPoC as detailed in section 73 of the Act. This might include situations where the designated senior officer has spoken to the SPoC directly or reviewed advice from the SPoC which is included with the application.

4.29 Public authorities unable to call upon the services of an accredited SPoC should not seek to undertake the acquisition of communications data.

[19] Communications Data Strategy Group is able to offer additional advice to SPoCs where investigations or operations in their public authority are considering the acquisition of such data.

4.30 In circumstances where a CSP is approached by a person who cannot be authenticated as an accredited individual and who seeks to obtain data under the provisions of the Act, the CSP may refuse to comply with any apparent requirement for disclosure of data until confirmation of both the person's accreditation and their duties as a SPoC is obtained from the Home Office.

4.31 Public authorities are expected to provide SPoC coverage for all communications data acquisitions that they reasonably expect to make. Police forces, for example, would expect to deal with threat to life situations at any time and should ensure that a SPoC is always available in such circumstances.

4.32 The SPoC is an accredited individual trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC authentication identifier[20]. Details of all accredited individuals are available to CSPs for authentication purposes.

4.33 An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. This encourages the public authority to regulate itself. The SPoC provides objective judgement and advice to both the applicant and the designated senior officer. In this way the SPoC provides a 'guardian and gatekeeper' function ensuring that public authorities act in an informed and lawful manner.

4.34 Where a number of providers are involved in the provision of a communication service, consultation with the public authority's SPoC will determine the most appropriate plan for acquiring data though it is the designated senior officer who ultimately decides which of the CSPs should be given a notice. With the proliferation of modern communications media, including mobile telephony, internet communications, and social networks, and given that one individual can use many different forms of communications, the knowledge and experience of the SPoC in providing advice and guidance to the designated senor officer is significant in ensuring appropriateness of any action taken to acquire the data necessary for an investigation.

4.35 The SPoC[21] will, as appropriate:

- Assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data[22];
- Advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;
- Engage with applicants to develop and implement effective strategies to obtain communications data in support of operations or investigations;

---

[20] At the time of writing, the authentication identifier is a SPoC Personal Identification Number ('SPoC PIN').

[21] Advice and consideration given by the SPoC in respect of any application may be recorded in the same document as the application and/or authorisation.

[22] In the event that the required data is inextricably linked to, or inseparable from, other events data, the designated senior officer must take that into account in their consideration of necessity, proportionality, collateral intrusion and unintended consequences.

- Advise on and manage the use of filtering arrangements, specifically in relation to progress of requests through the filter and compliance by the filter with the relevant authorisation;
- Advise applicants and designated senior officers on the interpretation of the Act, particularly whether an authorisation is appropriate;
- Provide assurance to designated senior officers that authorisations are lawful under the Act and free from errors;
- Consider and, where appropriate, provide advice to the designated senior officer on possible unintended consequences of the application;
- Provide assurance to CSPs that authorisations and notices are authentic and lawful;
- Assess whether communications data disclosed by a CSP in response to a notice fulfils the requirement;
- Assess whether communications data obtained by means of an authorisation fulfils the requirement of the authorisation;
- Assess any cost and resource implications to both the public authority and the CSP of data requirements; and
- Provide advice to the applicant and designated senior officer on when it may be appropriate to require use of the request filter in fulfilling an authorisation (see chapter 9 for more detail).

4.36 The SPoC would normally be the person who takes receipt of any communications data acquired from a CSP and would normally be responsible for its dissemination to the applicant. SPoCs in public authorities should be security cleared in accordance with their own organisation's requirements. When handling, processing, and distributing such information, SPoCs must comply with local security policies and operating procedures. Communications data acquired by public authorities must also by stored and handled in accordance with duties under the Data Protection Act[23].

4.37 Despite the name, in practice many organisations will have multiple SPoCs, working together. Nonetheless, in the course of a joint investigation between authority A with no SPoC and authority B with a SPOC and communications data acquisition powers, authority B may, where necessary and proportionate, acquire communications data under the Act to further the joint investigation.

4.38 For each individual application, the roles of SPoC and designated senior officers or SPoC and applicant will normally be carried out by two persons, depending on how a public authority uses its SPoCs. In exceptional cases, such as those covered under the urgent oral procedure or, on rare occasions, for security reasons, both roles may be carried out by the same person. Where specific, specialist units, particularly those involved in sensitive work, have undertaken streamlining to ensure better application of the principles of this code, these will generally be considered to be exceptional cases. One person may, in separate applications, carry out the roles of either the SPoC or the designated senior officer, or the roles of SPoC or the Applicant.

---

[23] See chapter 11 for further details of data protection safeguards.

4.39 The same person must never be both the applicant and the designated senior officer. Clearly, therefore, the same person should never be an applicant, a designated senior officer and a SPoC.

4.40 Any conduct to determine the CSP that holds, or may hold, specific communications data is not conduct to which the provisions of Part 3 apply. This includes, for example, establishing from information available to the public or, where necessary, from a service provider which provider makes available a specific service, such as a particular telephone number or an IP address.

4.41 Similarly Part 3 does not apply to any conduct by a public authority to obtain publicly or commercially available communications data. A Part 3 authorisation is not mandatory to obtain reference data[24], such as mobile phone mast locations, from a CSP as there is no intrusion with an individual's human rights. However, some reference data, such a details of Wi-Fi hotspots, may be commercially sensitive and a Part 3 authorisation can be sought by a public authority seeking to obtain this data from a CSP. Given the training undertaken by a SPoC and the on-going nature of a SPoCs engagement with CSPs, it is good practice to engage the SPoC to liaise with the CSP on such requests.

Exceptional circumstances

4.42 Section 73 provides for an authorisation to be granted without consultation with the SPoC in exceptional circumstances, which are limited to:

- The interests of national security; or
- Imminent threat to life or another emergency.

4.43 This provision does not absolve a public authority of the requirement to provide adequate SPoC cover for their investigative needs. The provision recognises that there may be some circumstances where, despite the best efforts of the public authority concerned, a SPOC is suddenly unavailable due, for example, to ill health. It is important that in such rare circumstances requests for communications data can be made in certain limited situations.

4.44 Organisations which are likely to deal with such cases should limit the risk that a SPoC is unavailable by entering into collaboration agreements where appropriate to do so.

4.45 There is a requirement to ensure that, in those cases where a SPoC is not available, the authenticity of the request can be or has been verified by the CSP. It is the responsibility of the public authority that considers such a process may be required to ensure that such a mechanism is in place.

4.46 In such cases the authorisation should record the reasons why SPoC coverage is not possible.

[24] See paragraph 2.24 for further information on reference data.

4.47 In all circumstances where public authorities do not consult a SPoC before an authorisation is granted, the senior responsible officer must notify the Commissioner of circumstances and reasons at the next inspection or as otherwise required by the Commissioner. CSPs should also record such instances and make these records available to the Commissioner on request. The details of the public authorities and the reasons such measures are being undertaken may be published and included in the Commissioner's report.

The senior responsible officer

4.48 Within every relevant public authority there should be a senior responsible officer. The senior responsible officer will be a person holding the office, rank or position of a designated senior officer within the public authority who may authorise access to communications data. The senior responsible officer is responsible for:

- The integrity of the process in place within the public authority to acquire communications data;
- Compliance with Part 3 of the Act and with this code;
- Oversight of the reporting of errors to the Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Commissioner's inspectors when they conduct their inspections; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the Commissioner.

Authorisations

4.49 An authorisation provides for persons within a public authority to engage in conduct, relating to a postal service or telecommunications system or data derived from such a telecommunication system, to obtain communications data. The following types of conduct may be authorised:

- Conduct to acquire communications data - which may include the public authority obtaining communications data themselves or asking any person believed to be in possession of or capable of obtaining the communications data to obtain and disclose it; or
- The issuing of a notice - allowing the public authority to require by a notice a telecommunications operator to obtain and disclose the required data.

4.50 An authorisation of conduct to acquire communications data may be appropriate where, for example:

- A CSP is not capable of obtaining or disclosing the communications data[25];
- There is an agreement in place between a public authority and a CSP relating to appropriate mechanisms for disclosure of communications data - in order to facilitate the secure and swift disclosure of communications data many CSPs have systems in place to ensure accurate and timely acquisition to communications data, while maintaining security and an audit trail;
- Where the data can be acquired directly from a telecommunication system and the activity does not constitute interception or equipment interference; or
- A designated senior officer considers there is a requirement to identify a person to whom a service is provided but a CSP has yet to be conclusively determined as the holder of the communications data.

4.51 An authorisation to issue a notice may be appropriate where a CSP is known to be capable of obtaining or disclosing the communications data (for further detail see paragraphs 4.67- 4.83).

4.52 Such an authorisation is not served upon a CSP, although there may be circumstances where a CSP may require or may be given an assurance that conduct being, or to be, undertaken is lawful. That assurance may be given by disclosing details of the authorisation or the authorisation itself. Where details of an authorisation are provided to a CSP in writing, electronically or orally, those details must additionally specify the manner in which the data should be disclosed and, where appropriate, provide an indication of any urgency or time within which the data need to be obtained.

4.53 Any designated senior officer in a public authority may only authorise persons working in the same public authority, or an authority which is a subscribing authority under a collaboration agreement, to engage in specific conduct, such as requesting the data via secure auditable communications data acquisition systems. This will normally be the public authority's or supplying authority's SPoC, though local authorities must now use the SPoC provided by the National Anti-Fraud Network (see chapter 6 for more details).

4.54 The decision of a designated senior officer whether to grant an authorisation shall be based upon information presented to them in an application.

4.55 Where an authorisation is granted under section 58(1)(b)(ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, the designated senior officer must be clear that it is also required for one of the purposes falling within section 58(7) and the application is proportionate to what is sought to be achieved.

4.56 An authorisation of conduct to acquire communications data must:

- Describe the conduct which is authorised and describe the communications data to be acquired by that conduct specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);

[25] Where possible, this assessment will be based upon information provided by the CSP.

- Specify the purpose for which the conduct is authorised, by reference to a statutory purpose under section 58(7) of the Act;
- Specify the office, rank or position held by the designated senior officer granting the authorisation. The name (or designation) of the designated senior officer granting the authorisation should also be recorded;
- Record the date and, when appropriate to do so, the time when the authorisation was granted by the designated senior officer;
- Confirm in writing that the designated senior officer has consulted a SPoC on this application;
- Specify where the communications data is to be obtained and disclosed by use of the request filter;
- If engaging the request filter, specify whether the processing of data (and its temporary retention for that purpose) is authorised and, if so, provide a description of the data that may be processed and the type or nature of processing to be performed (e.g. geographic correlation, IP address resolution);
- If engaging the request filter or requesting ICRs, specify whether any threshold for the number of results returned is set which would prevent any portion of records being disclosed;
- Where data is being sought from a CSP, specify whether the CSP may inform the subject(s) of the fact that an application has been made for their data; and
- Include a unique reference number.

4.57 In addition, an authorisation[26] to issue a notice must:

- Specify the operator to whom the notice applies and the nature of requirements to be imposed;
- Specify or describe the person(s) to whom the data is to be, or may be, disclosed or how to identify such person(s);
- Confirm whether a CSP may disclose the existence of this requirement, or any related pursuant request, to a customer or other individual;
- Specify whether the CSP may inform the subject(s) of the fact that an application has been made for their data; and
- Include a unique reference number and identify the public authority.

4.58 The original or a copy of the authorisation must be retained by the SPoC.

[26] Where the grant of an authorisation is recorded separately from the relevant application they should be cross-referenced to each other.

4.59 SPoCs and applicants should be mindful, when drafting authorisations within the meaning of section 58 of the Act, to ensure where possible the description of the required data corresponds with the way in which the CSP processes, retains and retrieves its data for lawful disclosure. CSPs cannot necessarily or reasonably edit or adapt their systems to take account of every possible variation of what may be specified in authorisations, particularly via communications data acquisition systems[27].

4.60 Requirements to identify a person to whom a service is, or has been, provided – for example telephone number subscriber checks – account for the vast majority of communications data disclosures. As a consequence of these requirements, some CSPs permit the lawful acquisition of this data by SPoCs, via secure auditable communications data acquisition systems. Where a SPoC has been authorised to engage in conduct to obtain details of a person to whom a service has been provided and concludes that data is held by a CSP from which it cannot be acquired directly, the SPoC may provide the CSP with details of the authorisation granted by the designated senior officer in order to seek disclosure of the required data.

4.61 It will often be appropriate to undertake the acquisition of entity data before obtaining related events data to confirm information within the investigation or operation.

4.62 However, where there is sufficient information within the investigation or operation to justify an application to obtain events data in the first instance, this may be undertaken. For example, in circumstances where:

- A victim reports receiving nuisance or threatening telephone calls or messages;
- A person who is subject of an investigation or operation is identified from high-grade intelligence to be using a specific communication service;
- A victim, a witness or a person who is subject of an investigation or operation has used a public payphone[28];
- A person who is subject of an investigation or operation is identified during an investigation (such as a kidnap) or from detailed analysis of data available to the investigator to be using a specific communication service;
- A mobile telephone is lawfully seized and communications data is to be acquired relating to either or both the device or its SIM card(s);
- A witness presents certain facts and there is a need to corroborate or research the veracity of those, such as to confirm the time of an incident they have witnessed; or
- An investigation of the allocation of IP addresses is needed to determine relevant subscriber information.

4.63 Where the acquisition of the entity data is required to assist an investigation or operation or for evidential purposes, that requirement can be included on an application for events data.

---

[27] The College of Policing Knowledge and Engagement Team (KET) (ketadmin@college.pnn.police.uk) can provide advice to SPoCs on how best to ensure up-to-date knowledge of data types.

[28] The telephone number and address of a public payphone is normally displayed beside it to assist persons making emergency calls to give their location to the emergency operator.

4.64 At the time of granting an authorisation of conduct to acquire communications data or to issue a notice in order to obtain specific events data, a designated senior officer may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of specific entity data relating to the events data to be obtained. This is relevant where there is a necessary and proportionate requirement to identify with whom a person has been in communication, for example:

- To identify with whom a victim was in contact, within a specified period, prior to their murder;
- To identify, where the target of an investigation or operation has been observed to make several calls from a public pay phone, the recipient of those calls;
- To identify a person making unlawful and unwarranted demands (as in the case of kidnap, extortion and blackmail demands and threats of violence); or
- Where a victim or a witness has identified a specific communication or communications and corroboration of facts may reveal a potential offender or other witness.

4.65 At the time of granting an authorisation of conduct to acquire communications data or to issue a notice in order to obtain specific events data, a designated senior officer may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of other events data. This is relevant where there is a necessary and proportionate requirement to identify a person from the events data to be acquired, and the means to do so requires the CSP or another CSP to query their events data information, for example:

- The CSP does not collect information about the customer within their customer information system but retains it in its original form as events data (such as a MAC or IMEI or an IP address); or
- Where evidence or intelligence indicates there are several CSPs involved in routing a communication and there is a requirement to establish the recipient of the communication.

4.66 It is the duty of the senior responsible officer to ensure that the designated senior officer, applicant or other person makes available to the SPoC such information as the senior responsible officer thinks necessary to ensure the integrity of any requirements for the acquisition of entity data to be obtained directly upon the acquisition or disclosure of any events data, and their compliance with Part 3 and with this code[29].

Notices

4.67 The giving of a notice is appropriate where a CSP is able to retrieve or obtain specific data, and to disclose that data, and the relevant authorisation has been granted. A notice may require a CSP to obtain any communications data, if that data is not already in its possession.

[29] Ordinarily the applicant or other person within the investigation or operation will prepare a schedule of data, for example telephone numbers, to enable the SPoC to undertake the acquisition of subscriber information. The schedule will include details of the person who prepared it, cross reference it to the relevant notice or authorisation and specify the events data from which the data are derived.

4.68 The decision of a designated senior officer whether to authorise the issuing of a notice shall be based on information presented to them in an application.

4.69 Once the designated senior officer has authorised that a notice should be given, it will be served upon a CSP in writing[30] or, in an urgent situation, communicated to the CSP orally.

4.70 The notice should contain enough information to allow the CSP to comply with the requirements of the notice.

4.71 A notice must:

- Be given in writing or, if not, in a manner that produces a record, within the public authority, of its having been given;
- Describe the communications data to be obtained or disclosed under the notice specifying, where relevant, any historic or future date(s)and, where appropriate, time period(s);
- Specify the requirements being imposed and the telecommunications operator on whom the requirements are being imposed;
- Where appropriate, provide an indication of any urgency or time within which the CSP is requested to comply with the requirements of the notice;
- Specify the purpose for which the notice has been given, by reference to a statutory purpose under section 58(7) of the Act;
- Include an explanation that compliance with the notice is a requirement of the Act unless the notice is cancelled. A CSP which has not complied before the period of validity for the authorisation expires is still required to comply. The notice should contain sufficient information including the contact details of the SPoC to enable a CSP to confirm the notice is authentic and lawful;
- Specify the manner in which the data should be disclosed and specify or describe the person(s) to whom the data is to be, or may be, disclosed or how to identify such person(s);
- Specify whether the data to be disclosed will pass through the filtering arrangements;
- Specify whether any threshold for the number of results returned is set which would prevent any portion of records being disclosed;
- Specify the office, rank or position held by the designated senior officer giving the notice. The name (or designation) of the designated senior officer giving the notice should also be recorded;
- Record the date and, when appropriate to do so, the time when the notice was given by the designated senior officer;
- Specify whether the CSP may inform the subject(s) of the fact that an application has been made for their data; and
- Include a unique reference number and identify the public authority[31].

[30] 'In writing' can include, but is not limited to, letter, fax, email, or via a secure portal operated by the CSP.

4.72 The original or a copy of the notice must be retained by the SPoC.

4.73 A CSP is not required to do anything under a notice which it is not reasonably practicable for it to do[32].

4.74 In giving notice a designated senior officer may only require a CSP to disclose the communications data to the designated senior officer or to a specified person working within the same public authority or an authority which is a subscribing authority under a collaboration agreement. This will normally be the public authority's SPoC.

4.75 Ordinarily the CSP should disclose, in writing or electronically, the communications data to which a notice relates not later than the end of the period of ten working days from the date the notice is served upon the CSP.

4.76 If a CSP, having been given a notice, believes that in future another CSP is better placed to respond, they should approach the authority to inform them of their view after disclosing the relevant data that they hold.

Urgent oral giving of notice or grant of authorisation

4.77 In exceptionally urgent circumstances[33], an application for the grant of an authorisation may be made by an applicant, approved by a designated senior officer and either notice given to a CSP or an authorisation granted orally. Circumstances in which an oral notice or authorisation may be appropriate include:

- An immediate threat of loss of human life, or for the protection of human life, such that a person's life might be endangered if the application procedure were undertaken in writing from the outset - this may include those situations where, for example there is serious concern for the welfare of a vulnerable person including children at imminent risk of being abused or otherwise harmed;
- an exceptionally urgent operational requirement where, within no more than 48 hours of the notice being given or the authorisation being granted orally, the acquisition of communications data will directly assist the prevention or detection of the commission of a serious crime[34] and the making of arrests or the seizure of illicit material, and where that operational opportunity will be lost if the application procedure is undertaken in writing from the outset; or
- A credible and immediate threat to national security or a time-critical and unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost, if the application procedure were undertaken in writing from the outset.

---

31 This can be a code or an abbreviation. It could be that part of a public authority's name which appears in its e-mail address. For police services it will be appropriate to use the Police National Computer (PNC) force coding.

32 See section 63(3) of the Act. SPoCs, designated senior officers or CSPs may contact the KET if they require further advice on what is reasonably practicable in a particular circumstance.

33 There is a general undertaking by CSPs to respond outside of normal office hours where there is an immediate threat to life.

34 See section 239(1) of the Act.

4.78 The use of urgent oral process must be justified for each application within an investigation or operation. The fact that any part of an investigation or operation is undertaken urgently must not be taken to mean that all requirements to obtain communications data in connection with that investigation or operation be undertaken using the urgent oral process. It must be clear in each case why it was not possible, in the circumstances, to use the standard, written process.

4.79 When, in a matter of urgency, a designated senior officer decides, having consulted the SPoC, that the oral giving of a notice or grant of an authorisation is appropriate, that notice should be given or the authorised conduct undertaken as soon as practicable after the making of that decision.

4.80 Particular care must be given to the use of the urgent oral process. When authorisation is given orally, the SPoC, when relaying service of the oral authorisation to the CSP, must make a note of the time, provide a unique reference number for the notice, provide the name (or designation) of the designated senior officer and the name and contact details of the SPoC and, if required by the CSP, their authentication identifier[35]. Where telephone numbers (or other identifiers) are being relayed, the relevant number must be read twice and repeated back by the CSP to confirm the correct details have been taken.

4.81 Written notice must be given to the CSP retrospectively within one working day[36] of the oral authorisation being given. Failure to do so will constitute an error which may be reported to the Commissioner by the CSP and must be recorded by the public authority (see the section on errors in chapter 21, Keeping of records, for more details).

4.82 After the period of urgency[37], a separate written process must be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the SPoC shall collate details or copies of control room or other operational logs which provide contemporaneous records of the consideration given to the acquisition of data, decision(s) made by the designated senior officer and the actions taken in respect of the decision(s).

4.83 In all cases where urgent oral notice is given or authorisation granted, an explanation of why the urgent process was undertaken must be recorded.

---

[35] At the time of writing, this is the SPoC PIN, see footnote 19.

[36] Working day means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday in any part of the United Kingdom.

[37] In some instances where life is at risk, for example in kidnap investigations, the period of urgency may be prolonged.

5 Duration, renewals and cancellations

Duration of authorisations and notices

5.1 An authorisation becomes valid on the date upon which authorisation is granted. It is then valid for a maximum of one month[38]. This means the conduct authorised should have been commenced or the notice served within that month.

5.2 Any notice issued under an authorisation remains in force until complied with or until the authorisation under which it was issued is cancelled (see paragraph 5.9).

5.3 All authorisations should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s)[39]. Any period should be clearly indicated in the authorisation. The start date and end date should be given, and where a precise start and end time are relevant these must be specified[40]. Where the data to be acquired or disclosed is specified as 'current', the relevant date should be taken to be the date on which the authorisation was granted by the designated senior officer. There can be circumstances when the relevant date or period cannot be specified other than 'the last transaction' or 'the most recent use of the service'.

5.4 Where an authorisation relates to the acquisition or obtaining of specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date upon which the authorisation was granted.

5.5 Designated senior officers should specify the shortest possible period of time for any authorisation. To do otherwise would impact on the proportionality of the authorisation and impose an unnecessary burden upon the relevant CSP(s).

Renewal of authorisations and notices

5.6 Any valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation. A renewed authorisation takes effect upon the expiry of the authorisation it is renewing.

5.7 Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasoning for seeking renewal should be set out by an applicant in an addendum to the application upon which the authorisation being renewed was granted.

---

[38] Throughout this code, a month means a period of time extending from a date in one calendar month to the date one day before the corresponding or nearest date in the following month. For example, a month beginning on 7 June ends on 6 July; a month beginning on 30 January ends on 28 February or 29 February in a leap year.

[39] For example, details of events data on a specific date or for a specific period or the details of a subscriber on a specific date or for a specific period.

[40] In the case of IP data, any timings should include an explicit indication of which time zone applies to those timings.

5.8 Where a designated senior officer is granting a further authorisation to renew an earlier authorisation[41], the designated senior officer should:

- Have considered the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated; and
- Record the date and, when appropriate to do so, the time when the authorisation is renewed.

Cancellation of authorisations and notices

5.9 A designated senior officer who has granted an authorisation under section 58(2) of the Act must cancel it if, at any time after the granting of the authorisaitone[42], it is no longer necessary for a statutory purpose or the conduct required by the authorisation is no longer proportionate to what was sought to be achieved. An authorisation may otherwise be cancelled at any time.

5.10 It may be the case that it is the SPoC or the applicant who is first aware that the authorisation is no longer necessary or proportionate. In such cases the SPoC (having been contacted by the applicant, where appropriate) may cease the authorised conduct, and then inform the designated senior officer who granted the authorisation

5.11 A notice issued under an authorisation (and any requirement imposed by a notice) is cancelled if the authorisation is cancelled but is not affected by the authorisation ceasing to have effect at the end of one month period of validity. Reporting the cancellation of a notice to a CSP should be undertaken by the designated senior officer directly or, on that person's behalf, by the public authority's SPoC. Where human rights considerations are such that a notice should be cancelled with immediate effect the designated senior officer or the SPoC will notify the CSP[43].

5.12 Cancellation of a notice reported to a CSP must:

- Identify, by reference to its unique reference number, the notice being cancelled; and
- Record the date and, when appropriate to do so, the time when the notice was cancelled.

5.13 In cases where the SPoC has initiated the cancellation of a notice and reported the cancellation to the CSP, the designated senior officer must confirm the decision for the SPoC either in writing or, if not, in a manner that produces a record of the notice having been cancelled by the designated senior officer. Where the designated senior officer who gave the notice to the CSP is no longer available, this duty should fall on a person who has temporarily or permanently taken over the role of the designated senior officer.

---

41 This can include an authorisation that has been renewed previously.

42 This can include a renewed authorisation.

43 If the authorisation being cancelled relates to an urgent operational situation that has been resolved, or has changed, it may be appropriate for the senior officer dealing with the situation, on the ground or in a control room, to notify the CSP (or arrange for their notification) that the notice imposed under an authorisation is cancelled where that person has the earliest opportunity to do so.

5.14

5.15 Cancellation of an authorisation should:

- Identify, by reference to its unique reference number, the authorisation being withdrawn;
- Record the date and, when appropriate to do so, the time when the authorisation was cancelled; and
- Record the name and the office, rank or position held by the designated senior officer informed of the withdrawal of the authorisation.

5.16 When it is appropriate to do so, a CSP should be advised of the cancellation of an authorisation, for example where details of an authorisation have been disclosed to a CSP.

6 Further restrictions and requirements in relation to applications

Communications data involving certain professions

6.1 The fact a communication took place does not disclose what was discussed, considered or advised.

6.2 However the degree of interference with an individual's rights and freedoms may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament[44], or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.

6.3 Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken by designated senior officers when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application.

6.4 Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That such an application has been made must be recorded (see chapter 21 on keeping of records for more details), including recording the profession, and, at the next inspection, such applications should be flagged to the Commissioner.

Applications for communications data relating to journalists and their sources

6.5 Issues surrounding the infringement of the right to freedom of expression may arise where an application is made for the communications data ofan identified or suspected journalist, an identified source or a suspected source of journalistic information and particularly, but not solely, where that application is for the purpose of identifying or confirming the identity or role of an individual as a journalist's source.

6.6 There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously.

[44] References to a Member of Parliament include references to a Member of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

6.7 A source of journalistic information is an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used. Throughout this code, references to sources should be understood to include any person acting as an intermediary between a journalist and a source.

6.8 An assessment of whether someone is a journalist (for the purposes of the Act) should be made on all the facts and circumstances available at that time. Consideration should be given, in particular, to the frequency of an individual's relevant activities, the level of professional rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest.

6.9 Where a designated senior officer is unclear as to whether an individual may be considered to be a journalist they should seek advice before authorising a relevant application (see para 6.15).

6.10 Applications for communications data in relation to journalists and their sources may still be made but applicants and designated senior officers will want to take particular care in considering such applications. To ensure that an application made to acquire communications data relating to a journalist or source is lawful it is crucial that public authorities apply correctly the process set out in this chapter.

6.11 The acquisition of communications data under Part 3 of the Act will be a justifiable interference with an individual's human rights under Articles 8 (right to respect for private and family life) and, in certain circumstances, 10 (freedom of expression) of the European Convention on Human Rights only if the conduct being authorised or required to take place is necessary, proportionate and in accordance with law.

6.12 Where an application is intended to identify or confirm the identity or role of an individual as a source of journalistic information judicial approval of the authorisation must be sought prior to the acquisition of the communications data taking place, other than where an exception applies. Where an application is not intended to identify or confirm the identity or role of an individual as a source of journalistic information judicial approval is not required but care should be taken.

6.13 Communications data alone may not be sufficient to identify a source - consequential action and other information is likely to be required. Identifying communications addresses does not in itself provide sufficient information to determine the nature of a relationship. However, where such requests are made with the intention that the information obtained will be used as part of an assessment of the identity of a source, this will require judicial commissioner authorisation.

6.14 The process for and guidance on both scenarios is set out in the following paragraphs.

6.15 Where appropriate public authorities should seek advice on the application of these provisions from the Home Office, the Investigatory Powers Commissioner and their own legal team. In addition, where an application may be considered novel or contentious public authorities should refer the matter to a Judicial Commissioner to review before deciding whether to authorise the application (see paras 6.34 onwards).

Applications to identify or confirm the identity or role of an individual as a source of journalistic information

6.16 Public authorities will, in very limited circumstances, have a legitimate need to acquire communications data to identify or confirm the identity or role of an individual as a journalist's source. In such circumstances issues surrounding the infringement of the right to freedom of expression are likely to arise. Public authorities must consider whether there is another overriding public interest which justifies any interference with this right.

6.17 Where a designated senior officer has granted an authorisation for this purpose in circumstances other than in relation to an immediate threat to life (see below) the authorisation will not take effect until such time as a Judicial Commissioner has approved it under section 74 of the Act.

6.18 In deciding whether to approve an authorisation to identify or confirm the role of an individual as a journalistic source a Judicial Commissioner must, among other matters, have regard to the public interest in protecting a source of journalistic information and consider that there is another overriding public interest before approving an authorisation.

6.19 In considering whether an application is being made for the purpose of identifying or confirming the identity or the role of an individual as a journalist's source, public authorities should pay particular consideration to applications relating to communications addresses of:

- persons identified as or suspected to be a source;
- persons identified as or suspected to be acting as an intermediary between a journalist and an identified or suspected source; and
- person identified as or suspected to be a journalist.

6.20 In addition to applications specifically intended to identify a journalist's source, the acquisition of communications data to confirm existing understanding or corroborate other evidence of the identity of, or role of an individual as, a journalist's source requires judicial authorisation.

6.21 The requirement for judicial authorisation applies to an authorisation made for the purpose of identifying or confirming any identifying characteristic of a source, not solely their name. For instance, in certain circumstances it may not be the name of a source that is being sought but other identifying characteristics such as their home location or occupation.

6.22 Designated senior officers should apply careful consideration before authorising the acquisition of communications data to identify or confirm who within a public authority may have leaked information to the media. Such an application should only be made where it is considered that there is a public interest in making such an application which overrides the public interest in source protection. Judicial authorisation is required. This includes situations where the passing of any information may in itself constitute a crime.

6.23 In addition to the requirements detailed in chapter 4, an application to acquire communications data for the purpose of identifying or confirming the role of an individual as a source should give special consideration to necessity and proportionality and specifically draw attention to the following matters:

- **Potential infringements of rights**: The existence of any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and freedom of expression.

- **Public interest in source protection**: Consideration of whether the intrusion is justified, giving proper consideration to whether the public interest is best served by the application. The application should consider properly whether the suspected conduct is of a sufficiently serious nature for rights to freedom of expression to be interfered with.

- **Collateral intrusion**: As well as consideration of the rights of the individual under investigation, consideration should also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. Any potential for unintended consequences of such applications should be considered.

6.24 It will not be sufficient to simply state, without any further detail on how the matters apply in the case and any mitigations put in place that the matters have been appropriately considered.

6.25 Each authority must keep a central record of all occasions when such an application has been made, including a record of the considerations undertaken (see chapter 21 on keeping of records for more details). At the next inspection, such applications should be specifically flagged to the Commissioner.

6.26 An authorisation made for the purpose of identifying or confirming the role of an individual as a journalist's source cannot take effect until such time as a Judicial Commissioner has approved it, except where an authorisation is not required due to an imminent threat to life

Threat to life exception

6.27 In very limited circumstances an authorisation made for the purpose of identifying or confirming the identity or role of an individual as a journalist's source will not require judicial approval. If, and only if, there is believed to be an immediate threat of loss of human life, such that a person's life might be endangered by the delay inherent in the process of judicial authorisation, law enforcement agencies may continue to use the existing internal authorisation process under the Act.

6.28 Examples of situations in which judicial approval may not be required due to an immediate threat to loss of human life include:

- a warning of an imminent terrorist incident being telephoned to a journalist or newspaper office;

- a journalist conducting an investigation which includes a significant element of personal danger who has not checked in with his office at the agreed time; or

- a source contacting a journalist to reveal their intention to commit suicide.

6.29 Such applications must be notified to the Commissioner as soon as reasonably practicable, as agreed with the Commissioner.

6.30 If additional communications data is later sought for the purpose of identifying or confirming the identity or the role of an individual as a journalist's source as part of the same investigation, but where a threat to life no longer exists, judicial approval should be sought.

Applications relating to journalists which are *not* to identify or confirm the identity or role of an individual as a source of journalistic information

6.31 The requirement for judicial oversight does not apply where applications are made for the communications data of those known or suspected to be journalists or sources but where the application is not to identify or confirm the role of an individual as a source of journalistic information.

6.32 The following paragraphs provide examples of when an application relating to a journalist or their source may be considered not to be for the purpose of identifying or confirming the role of an individual as a journalist's source. In each case, public authorities should apply their own assessment to the specific circumstances of the case and identify whether there is any potential additional infringement of rights or intrusion to be considered, including whether the application should be considered novel or contentious (see para 6.34).

- Where the journalist is a victim of crime and it is clear that their profession and sources are not relevant to the investigation, judicial approval may not be required.

- Where an identified source or suspected source is a victim of crime and it is clear that their role as a source is not relevant to the investigation, judicial approval may not be required.

- Where a journalist, identified source, or suspected source is a witness or other by-stander in an investigation not related to their roles as journalist or source and a communications data application is made to discount them from the investigation, judicial approval may not be required.

- Where the journalist, identified source, or suspected source is suspected of committing a crime, judicial approval may not be required in all circumstances:

    - For instance, where a journalist is suspected of committing a crime and it is clear that their profession and sources are not relevant to the investigation, judicial approval may not be required.

    - Additionally, it may be necessary to acquire the communications data of a known criminal under investigation who is also a source. Where a

journalist-source relationship is already confirmed and the individual's role as a source is not relevant to the investigation, judicial approval may not be required.

- Where an individual on the witness protection programme is concerned that an unsolicited caller is a journalist, or other individual, hoping to sell a story about the individual's new identity, judicial approval may not be required.

- Where an investigation is conducted to prove criminal conspiracy between a journalist and their source, and the journalist-source relationship is already confirmed, judicial approval may not be required in all circumstances. For example, where specific facts about the timing or location of communications between the two individuals must be confirmed to prove the criminal conspiracy, judicial approval may not be required.

6.33 An application for communications data relating to a known or suspected journalist or a known or suspected source, which is not to identify or confirm the identity or role of an individual as a journalist's source, may still have an unusual degree of sensitivity attached to it. Where this is the case the application should be considered potentially contentious and referred to the Judicial Commissioner for review.

6.34 Applications which should be considered to fall into this category and should therefore be referred to the Judicial Commissioner include, but are not limited to, applications for communications data of a journalist or their source which are not to identify or confirm the identity or role of an individual as a journalistic source and:

- Will likely result in the incidental and unintended identification or confirmation of a source (collateral intrusion into journalist sources) yet may still be justified; or

- Relate to an investigation involving whistle-blowing or the leaking of documents or information to the media. An application for the purpose of limiting reputational damage would not meet a statutory purpose and so would not be considered lawful.

6.35 An example of collateral intrusion into a journalist's source may be where:

- subscriber checks are requested for all communications addresses in contact with a journalist over a period of time because, for instance, they are a victim of a serious crime; and

- those checks are not for the purpose of identifying or confirming a source; and

- information is already known about a source run by that journalist which will unavoidably result in the identification of that source if subscriber checks are obtained.

6.36 Particular care should therefore be taken to ensure that the application considers whether the intrusion is justified, giving proper consideration to the public interest. As well as consideration of the rights of the individual under investigation, consideration should also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. Any potential for unintended consequences of such applications should be considered.

Novel and contentious acquisition

6.37 In recognition of the capacity of modern communications data to produce insights of a highly personal nature, where it is considered that a communications data application is novel or contentious, the senior responsible officer must refer the matter to a Judicial Commissioner for advice before deciding whether to authorise the application. A referral to the Judicial Commissioner may relate to a single application or to an issue of principal arising in an application.

6.38 Where appropriate the senior responsible officer should discuss with the Commissioner particular circumstances which might cause a case to be considered novel and contentious for that public authority. An application for communications data might be considered novel and contentious for one public authority but not another.

6.39 The following examples might be considered novel or contentious:

- New technical methods of acquisition;
- New types of communications data;
- Applications which might result in an unusual amount of collateral intrusion but still be considered proportionate; and
- Where there might be unusual sensitivity attached to the application regarding the nature of the target.

6.40 For guidance on how applications for communications data relating to a journalist or their source may be considered novel or contentious, please see para 6.34.

6.41 Where the designated senior officer or senior responsible officer is in any doubt regarding whether an application is novel or contentious they should consult the Commissioner before deciding whether to seek advice on such a case.

6.42 In urgent cases, such as threat to life or the interests of national security in a particular investigation, it may not be possible to seek the opinion of the Commissioner in advance of making an application for the data. In such circumstances the public authority should seek retrospective advice as soon as possible and take this into account in future applications of a similar nature.

6.43 The public authority must record the views of the Judicial Commissioner and where the designated senior officer proceeds against the recommendation of the Judicial Commissioner must give his reasons for doing so.

6.44 The views of the Judicial Commissioner on such cases should be recorded and may be shared between public authorities to inform consideration of future applications.

Public authority collaboration agreements

6.45 Any public authority may participate in a collaboration agreement, by which the designated senior officer and other officers of the supplying authority are put at the disposal of the subscribing authority. In practice, the subscribing authority will most commonly make use of a partner's designated senior officer and SPoC. A public authority may be directed to enter into such an agreement by the Secretary of State. All local authorities must make applications through a SPoC at the National Anti-Fraud Network ('NAFN') (see paragraph 6.51).

6.46 Before entering into a collaboration agreement, all parties to the agreement should consider whether:

- Sufficient alignment exists between the parties to allow the supplying authority to meet the specific needs of the subscribing authority, for instance provision of out-of-hours services or specific security clearances;
- The supplying authority is sufficiently familiar with the subscribing authority's role to be able to provide relevant expertise; and
- The length of time the collaboration agreement will last for, for instance whether the agreement is just for the duration of a particular operational requirement.

6.47 When deciding whether to direct a public authority to enter into a collaboration agreement the Secretary of State will consider:

- The issues identified in paragraph 6.46;
- The number and nature of authorisations made by a public authority; and
- The nature and function of the public authority concerned.

6.48 In granting authorisations on behalf of the subscribing authority, the designated senior officer at the supplying authority must ensure that in accordance with the provisions under Schedule 4 of the Act:

- Authorisations are only granted to the subscribing authority for the purposes for which that authority may acquire communications data; and
- The designated senior officer holds the relevant minimum rank or position detailed for the subscribing authority

6.49 Any collaboration agreement between public authorities must be undertaken in writing or, if not, in a manner that produces a record within the relevant public authorities. This agreement, or the fact of its existence, must then be published along with any other details considered appropriate and the Commissioner notified.

Local authority procedures

6.50 NAFN provides shared SPoC services to local authorities. Local government legislation allows for NAFN to act on behalf of local authorities within England and Wales, Scotland and Northern Ireland for certain functions[45].

6.51 In accordance with section 71 all local authorities who wish to acquire communications data under the Act are required to become members of NAFN and use their shared SPoC services. This means that applicants within local authorities are required to consult a NAFN SPoC throughout the authorisation process, including before referring the case to a designated senior officer for approval. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to applicants and designated senior officers ensuring the local authority acts in an informed and lawful manner.

6.52 In addition, local authority applications for communications data require judicial approval under section 72 of the Act. Judicial approval must be requested once all the internal authorisation processes have been completed, including consultation with a NAFN SPoC, but before the SPoC requests the data from the CSP. In England, Wales and Northern Ireland the authorisation must be provided by a magistrate; in Scotland a sheriff or summary sheriff.

6.53 The local authority, rather than NAFN, is responsible for submitting the application for judicial authorisation. It is for the local authority to decide on the most appropriate representative to present their application to the magistrate or sheriff. The judicial application must include relevant documentation, including the original Act authorisation or notice. Once the case has been heard, the magistrate or sheriff will complete a judicial order outlining their decision. Should authorisation be granted, the local authority will provide the judicial order to the NAFN SPoC.

6.54 Where a local authority seeks communications data for the purposes of identifying or confirming a journalistic source the requirement to seek local magistrate approval under section 72 does not apply. Instead the local authority must apply to the Judicial Commissioner for approval of the authorisation under section 74.

6.55 A local authority may not grant an authorisation requiring the processing or disclosure of internet connection records for any purpose (see chapter 7).

[45] The Local Government Act 1972; Local Government Act (Scotland) 1973; and Local Government Act (Northern Ireland) 2014.

7 Considerations in relation to the acquisition of internet data

Internet connection records

7.1 In addition, under certain circumstances, a designated senior officer may grant an authorisation to obtain data which constitutes or requires the processing or disclosure of an internet connection record (ICR) (see paragraph 2.62 for the definition of an ICR). Subject to paragraph 2.28 any application that involves the disclosure of ICRs must be authorised as events data.

7.2 All existing requirements regarding necessity and proportionality for authorisations to obtain communications data also apply to the acquisition of ICRs. However, in addition, particular care must be taken by designated senior officers when considering such applications, including additional consideration of the proportionality of the application in relation to the level of processing, where known, and disclosure involved.

7.3 Section 59 of the Act recognises the additional sensitivities associated with ICRs and restricts public authority access accordingly. A public authority can therefore only require the disclosure or processing of internet connection records for the purpose of identifying:

- The sender of an online communication (either the device or the person);
- The internet communications services[46] an individual is using, such as messaging applications;
- The internet services[47] an individual is using which wholly or mainly involve making available or acquiring material, whose possession is a crime – for example child abuse imagery or illicit drugs; or
- Other internet services an individual is using – for example to book travel or look at online mapping services.

7.4 An application to acquire ICRs may relate to one or more of these 'investigative purposes'.

7.5 The Act applies important restrictions when the statutory purpose for which ICRs are acquired is for the prevention and detection of crime. In these circumstances ICRs can only be acquired:

---

[46] An internet communication service is a service which provides for the communication between one or more persons over the internet and may include email services, internet telephony services and web forums.

[47] An internet service is a service provided over the internet. It includes internet communication services, websites and applications.

- for the prevention and detection of crime where the offence, or one of the offences, is one for which a person is capable of being sentenced to imprisonment for a term of 6 months or more;

- for the prevention and detection of any other crime which would fall within the definition of serious crime in section 239 of the Act, - i.e. offences involving the use of violence, conduct that results in substantial financial gain and conduct by a large number of people in pursuit of a common purpose;

- where the conduct is an offence which can only be committed by a corporate body – for example corporate manslaughter - where a penalty of imprisonment does not apply; and

- where the conduct concerned involves, as an integral part of it, the sending of a communication or a breach of a person's privacy - for example cyber bullying and harassment offences and offences which are themselves invasions of privacy such as data protection offences of unlawfully acquiring personal information.

7.6 The crime threshold does not apply to applications made for the investigative purposes of identifying the sender of an online communication (section 59(3)). Such applications will not result in the disclosure of a list of internet connection records as the service used will already be known. A CSP could be asked a number of different questions, for example who was using this IP address at date/time, which of your customers has accessed this server at date/time or which of your customers conducted an activity of concern on a known website at a known date or time. The material disclosed will thus take the form of an IP address and related entity data, where available (see identifying the sender of an online communication in the next section).

7.7 Applications may be made by the public authority for the purposes of identifying:

- The communications service used by an individual;

- Internet services used to access or make available illegal material; or

- What other internet services a person is using.

7.8 Such applications will require a CSP to disclose of a list of internet connection records covering a specific time period. This will include ICRs not directly relevant to the investigation. Given the scope for collateral intrusion the designated senior officer will therefore need to apply careful consideration to ensure this period is proportionate and no longer than necessary.

7.9 Occasions when a public authority might seek ICRs to identify an internet communications service being used include:

- To facilitate follow up with another communications provider in order to establish who a missing person was in contact with before their disappearance;

- Where a person is known to be communicating online but it is not known how; or

- To facilitate follow up with another communications provider in order to identify contacts of a suspect following the seizing of a communication device.

7.10 An ICR is unlikely to identify who a person has been communicating with online or when they have been communicating. In most cases it will simply identify the services which a person has accessed allowing further enquiries to be made of the relevant provider.

7.11 A public authority might seek ICRs in order to identify possible access to illegal information when seeking, for instance, to identify whether a person seen viewing illegal images has been accessing sites containing this information, to identify whether a person suspected of owning illegal weapons has been accessing illegal online market places or to identify which website a person has uploaded illegal images.

7.12 A public authority might seek ICRs in relation to internet services more generally when seeking, for instance, to identify how a person who is suspected of people trafficking is making travel arrangements or to identify any activity which may assist in locating a missing vulnerable person. Any services accessed by an individual may provide leads for public authorities to pursue in their investigation by identifying travel services, mapping applications or other relevant avenues to follow up.

7.13 A public authority may only examine internet connection records returned to them which do not directly relate to the purpose for which they were acquired (for example a record of access to a travel site returned in response to a request for communication services) where necessary and proportionate to do so for the purposes set out in section 58(7) of the Act. For further information see paragraphs 21.37 - 21.39 on excess data.

7.14 Local authorities are prohibited from seeking the processing or disclosure of ICRs for any purpose.

7.15 There may be circumstances where it is more appropriate for public authorities to utilise the alternative lawful powers available to them, such as interception or equipment interference warrants, to obtain information which is similar to, or includes, ICRs. The use of these powers will be subject to higher levels of authorisation, requiring a warrant to be issued by the Secretary of State and approved by a Judicial Commissioner. Before using such powers the relevant authority must consider whether a less intrusive means of collecting such data is appropriate.

Identifying the sender of an online communication

7.16 Internet Protocol Address Resolution (IPAR) is necessary to identify the sender of an online communication, where the public authority is in possession of an IP address related to a communication of interest and needs to determine the associated user(s). In the current technological environment this is often not a simple task and applications to acquire communications data for this purpose must consider the associated complexities.

7.17 In order to communicate on the internet a device must be allocated an IP address. A communication may be between two users, in which case the IP address will normally relate to their personal electronic device, between two servers in which case the IP addresses will relate to the equipment in question, or between a user's personal electronic device and a server for instance a user downloading material from a website. The IP address from which the communication originated is the source IP address, that by which it is received is the destination IP address.

7.18 In order to enable the CSP to resolve an IP address the public authority must provide a minimum of one source IP address and one date/time. To enable the identification of a person who initiated a communication, rather than the service used to send that communication this must be a source IP which relates to a user's personal device not a server.

7.19 However, where IP addresses are shared between network customers as is commonly the case, provision of just the source IP address and the time of the communications will often not be sufficient to resolve the address to an individual. Public authorities should therefore ensure they use any other data that is available to them with the application. For example, if there are more IP addresses and times which they believe relate to the same suspect then that data should also be provided to the CSP. This includes the following types of data where available:

- Source and destination port numbers, both public and private;
- User equipment identifiers;
- Account reference details; and
- Service identifiers or web domains.

7.20 Where public authorities need to resolve IP addresses, internet connection record data will often be the only additional data that is available. This is because they will already know the internet service that has been used to send the relevant communication which they are trying to resolve. For example, if someone posts a bomb threat to an online blog, the blog's access records will provide the police with both the source IP address allocated to the user who posted the threat, as well as the destination IP address of the blog server. The police should provide both these IP addresses, plus any other information the blog records provide such as ports used, to the CSP as this will increase the likelihood that the CSP will be able to accurately match these details to an individual.

7.21 Network implementation of network address translation and dynamic IP addressing means that an IP address may only be allocated to a particular user in conjunction with other users, and sometimes for an extremely short period of time, particularly where allocated to mobile devices. A request for IPAR data may therefore return a large data set to the public authority. As a designated senior officer will not know in advance how large that return will be, it is important to consider the proportionality and potential collateral intrusion of such applications.

7.22 In addition to the standard authorisation procedure for communications data applications the following additional steps should be taken:

- The applicant should consider what data is available to them and base their application on those elements of data which will enable the CSP to make the most accurate and proportionate return;

- The applicant should use as many relevant identifiers as are available to them in making their application, in order to ensure that the CSP may make the most accurate return. Where more than one IP address or more than one date / time is available, the public authority should consider resolving more than one to allow cross-correlation of data sets;

- The designated senior officer must take account of advice provided by the SPoC as to an appropriate strategy for the acquisition of IPAR data in each case;

- The designated senior officer must consider, in making an application, whether to specify that the CSP should only return the data where it can be linked to one individual or whether larger data sets may be returned. The designated senior officer may decide to accept returns of larger data sets only where the necessity and proportionality case is sufficiently strong and must detail their considerations of proportionality in the authorisation; and

- The designated senior officer must give consideration to where returns of incomplete data could lead to false positives or false negatives for an operation and how this might be mitigated through the use of corroborating evidence. As a greater number of communications services become available, it is no longer possible to obtain full visibility of an individual's communications. Whilst the data available might only identify one individual who meets the specified criteria, the provision of further data regarding other communications methods might identify further matches, thus rendering the initial result a 'false positive'. The likelihood of 'false negatives' where individuals are ruled out of a case because they did not appear in a particular data set should also be considered.

7.23 The same considerations will apply where the public authority does not have an IP address but wishes to determine the individual that carried out a certain action online.

8 Special rules on the granting of authorisations and giving of notices in specific matters of public interest

Sudden deaths, serious injuries, vulnerable and missing persons

8.1 There are circumstances when the police undertake enquiries in relation to specific matters of public interest where the disclosure of communications data may be necessary and proportionate. Section 58(7) of the Act specifies certain purposes for which the acquisition and disclosure of communications data may be necessary. These purposes assist the police in carrying out its functions. For example:

- Identifying any person who has died or who is unable to identify himself because of a physical or mental condition, other than as a result of crime (for example in the case of a natural disaster or an accident);
- Obtaining information about the reason for a person's death or condition;
- Locating and notifying next of kin following a sudden or unexpected death;
- Locating and notifying next of kin of a seriously injured person; and
- Locating and notifying the next of kin or responsible adult of a child or other vulnerable person where there is a concern for the child's or the vulnerable person's welfare.

8.2 Often a telephone, telephone number or other communications details may be the only information available to identify a person or to identify their next of kin or a person responsible for their welfare.

8.3 Equally communications data can help establish the facts relevant to a person's death or serious injury, where no crime has occurred.

8.4 Under the Act communications data may also be obtained and disclosed in serious welfare cases where it is necessary within the meaning of section 58(7)(g) and the conduct authorised or required is proportionate to what is sought to be achieved by obtaining the data.

Public Emergency Call Service (999/112 calls)

8.5 The Act regulates the acquisition and disclosure of communications data for the statutory purposes in section 58(7). The Communications Act 2003 also requires certain CSPs to provide communications data to the emergency services following an emergency call made to 999 and 112 emergency numbers.

8.6 To assist the emergency services and emergency operator further details in relation to handling 999 and 112 calls are contained within the Public Emergency Communications Service Code of Practice.

8.7 This code is not intended to regulate the handling of an emergency call but to ensure the boundary between this code and the Public Emergency Communications Services Code of Practice is clear. In so doing this code recognises an emergency period of one hour after the termination of the emergency call in which disclosure of communications data to emergency services will largely fall outside the provisions of the Act.

8.8 CSPs must ensure that any service user can access the emergency authorities by using the emergency numbers and, to the extent technically feasible, make caller location information available to the emergency authorities for all 999/112 calls. In practice this means sufficient detail to identify the origin of the emergency call and, if appropriate, to enable the deployment of an emergency service to the scene of an emergency.

8.9 It is usual for CSPs to disclose, at the time of the call, some identity (caller line identity) and caller location information data (fixed or mobile) to the emergency services in order to facilitate a rapid response to the emergency call.

8.10 CSPs should take steps to assure themselves of the accuracy of the information they may be called upon to disclose. Any known limitations in this accuracy, particularly for location, should be proactively disclosed to the emergency services.

8.11 The emergency service can call upon an emergency operator or relevant service provider to disclose data about the maker of an emergency call within the emergency period within one hour of the 999/112 call.

8.12 It is appropriate for the emergency service or emergency operator to require the CSP to disclose any further caller location information that might indicate the location of the caller at the time of the emergency call. Within one hour of the 999/112 call, it is also appropriate for the CSP, acting in the belief that information might assist the emergency service to respond effectively or efficiently to the emergency, to proactively disclose to the emergency service or emergency operator any further caller location information (CLI) about the location of the caller at the time of the emergency call.

8.13 If an emergency call is disconnected prematurely for any reason, technical or otherwise, and the emergency operator is aware or is made aware of this, then the emergency operator can elect to represent the data disclosed when the call was put to the emergency service initially. This voluntary disclosure would fall outside the scope of the Act.

8.14 Some CSPs have provided secure auditable communications data acquisition systems for the disclosure of communication data under the Act. Where these exist, it is appropriate for emergency services to be provided with accreditation details to use them for acquiring data about the maker of an emergency call or caller location information, as appropriate, during the emergency period.

8.15 When a secure auditable system is not available, a manual application for data can be made. The Public Emergency Communications Service Code of Practice contains the process to be followed[48].

8.16 If the emergency call is clearly a hoax, there is no emergency. Where an emergency service concludes that an emergency call is a hoax and the reason for acquiring data in relation to that call is to detect the crime of making a hoax call – and not to provide an emergency service – then the application process under the Act must be undertaken.

8.17 Should an emergency service require communications data relating to the making of any emergency call after the expiry of the emergency period of one hour from the termination of the call, that data must be acquired or obtained under the provisions of the Act.

8.18 Where communications data about a third party (other than the maker of an emergency call) is required to deal effectively with an emergency call, the emergency service may make an urgent oral application for the data. Disclosure of that data would also fall within under the provisions of the Act.

8.19 Increasingly, members of the public are using non-emergency numbers to request assistance.

8.20 A caller might dial either 101 or 111 to seek non-emergency assistance (or Crimestoppers on 0800 555 111 should they wish to report crime anonymously). In the case of calls to 101, 111 and other relevant non-emergency assistance services, the call handler might believe it is more appropriate that an emergency response is made[49]. If insufficient details are available to provide an emergency response it is appropriate for the call handler to seek assistance using the 999/112 numbers if that act would speed up the provision of emergency assistance. If necessary, it is also appropriate for the call handler to contact a CSP to seek sufficient subscriber or other communications data, as are necessary and appropriate to assist with the provision of an emergency response.

8.21 The Act does not seek to regulate either the actions of the call handler or the provision of data by the CSP.

---

[48] To be used with the Public Emergency Communications Service Code of Practice, there is a guide specifically for emergency operators and emergency authority control room staff on when it is appropriate to contact CSPs.

[49] Guidance regarding non-emergency numbers is available from the KET (ketadmin@college.pnn.police.uk). It sets out what records need to be retained so that audit and oversight activities can take place. This emergency process is not to be used in support of activity to investigate hoax or malicious callers or for other situations where the call handler does not have a belief that an emergency situation has arisen. Where a call starts as a non-emergency but develops into an emergency call then paragraphs 8.12 would apply.

Malicious and nuisance communications

8.22 Many CSPs offer services to their customers to deal with complaints concerning malicious and nuisance communications. Although these services vary, all CSPs believe that such calls can be very distressing for their customers and that every effort should be made to resolve such situations as efficiently and effectively as possible.

8.23 The victim of malicious or nuisance communications may, in the first instance, bring it to the attention of their CSP or report it to the police.

8.24 When contacted directly by a customer, the CSP may consider the circumstances of the complaint are such that the customer should be advised to report the matter without delay to the police for investigation.

8.25 Additionally the CSP can offer practical advice on how to deal with nuisance communications and may, for example, arrange a change of telephone number. The advice given by the CSP may indicate that the circumstances could constitute a criminal offence. The CSP may choose to disclose data to its customer relating to the source of the malicious or nuisance communications, but must ensure that the disclosure complies with the provisions of both the DPA and the Privacy and Electronic Communications Regulations (2003).

8.26 Upon receipt of a complaint a CSP may retrieve and retain relevant specific data that, if appropriate, can be disclosed to the police later. If the complainant wishes the matter to be investigated, it is essential for the CSP and the police[50] to liaise with one another to ensure the lawful disclosure of data to enable any offence to be effectively investigated.

8.27 Where the complainant reports a matter to the police that has been previously raised with the CSP, any data already collated by the CSP may be disclosed to the police SPoC under the provisions of the DPA or the Privacy Regulations[51]. Subsequent police investigation may require the acquisition or disclosure of additional communications data from the complainant's CSP or other CSPs under the provisions of the Act.

8.28 Whether the initial complaint is reported to the CSP or directly to the police, careful consideration should be given to whether the occurrence of malicious or nuisance communications are, or may be, related to other incidents or events. Specifically, this could be where the complainant is a victim of another crime or is a witness or a member of a trial jury in ongoing or forthcoming criminal proceedings.

[50] Ordinarily this will be overseen and coordinated by the police force's SPoC.

[51] Regulation 15 concerns tracing of malicious or nuisance calls.

9 The request filter

9.1 The request filter will provide an additional safeguard on the acquisition of communications data. It will work alongside other acquisition safeguards and existing infrastructure to limit the volume of communications data being provided to a public authority.

9.2 Only specified communications data defined in an authorisation will be processed by the request filter. The specified data must be necessary and proportionate for the operational requirement set out in the authorisation and can only operate on limited sets of authorised data using specified processing patterns. The request filter will only retain communications data temporarily whilst the data is being processed. Once processing is complete the data will be deleted.

9.3 The request filter is available to all public authorities to assist in obtaining the communications data that they are permitted to use, subject to individual authorisations. It will support complex communications data investigations where multiple sets of data need to be correlated. The filter will assist public authorities by:

- Providing a mechanism for pulling fragmented communications data together and providing a more complete analysis. With the increasing use of a wider range of online communications services and communications networks, the communications data required to answer operational questions is becoming more fragmented;

- Reducing analytic burden on public authorities and getting an operational answer in the shortest possible time to facilitate the timely recovery of forensic evidence, eliminate individuals without further more intrusive activity, and identify witnesses while events remain fresh in their memories; and

- Managing proportionality and collateral intrusion. A public authority will only be provided with the data that directly answers its question, as opposed to all the data originally required to conduct the analysis.

9.4 The request filter will be available to all public authorities. The SIA can acquire data in bulk under the provisions in part 6 of the Act and select that data for examination for operational purposes specified in the warrant. In considering whether a bulk warrant is necessary and proportionate, the Secretary of State and Judicial Commissioner must take into account whether the information it is considered necessary to obtain under the warrant could reasonably be obtained by other means. This consideration should include whether the required information could reasonably be obtained through a less intrusive power such as the targeted acquisition of communications data or the targeted acquisition of communications data using the request filter.

Authorisations

9.5 The request filter can be used to obtain and process data as part of a targeted communications data authorisation.

9.6 During the development of an application, the SPoC may advise applicants of situations where it would be appropriate to make use of the request filter and its capabilities in order to manage collateral intrusion.

9.7 The request filter may be identified as part of the approach to managing collateral intrusion in an authorisation. The request filter will only disclose records that match specified criteria to the SPoC and applicant. In making such a case, the authorisation should consider the likely effectiveness of the specified criteria in achieving the expected reduction in records. For example if the question to the request filter is 'who was in location A at time N and location B at time M', effectiveness will depend on, for example, the distance between the locations and any links between the locations such as main roads and railway lines.

9.8 The designated senior officer, with advice from the SPoC, and taking account of information provided by the request filter on the volumes of data that may be disclosed, should consider the proportionality of:

- The data to be disclosed to the request filter by the CSPs; and
- The data to be disclosed to the applicant by the request filter.

9.9 Consideration of proportionality for authorisations involving the request filter should take into account future evidential requirements. Particular consideration should be given as to whether it will be possible to evidence any records disclosed by the request filter through secondary communications data authorisations or other means. For example, if the question to the request filter is 'who was in location A at time N and location B at time M', it may be possible to evidence that any individuals identified were indeed in the specified locations through a secondary communications data authorisation seeking the locations of those identified individuals at times N and M.

9.10 The authorisation should also consider the proportionality of the data to be disclosed to the request filter by the CSPs, even if the majority is not expected to be released to the public authority.

9.11 As with other authorisations, the designated senior officer may place constraints on the release of any results from the filter so that if the number of results is greater than expected, disclosure to the public authority will be prevented.

Making use of the request filter

9.12 The SPoC is responsible for monitoring the request filter progress and managing compliance with the relevant authorisation.

9.13 The request is sent to the filter which in turn identifies the relevant communication service providers for the request and requires them to disclose the authorised communications data only to the request filter. They will not be aware of the detail of the processing to be undertaken.

9.14 Depending on the nature of the communications data and processing, the request filter may require decisions to be made by the SPoC during the processing. For example if there is a delay with one of the data sources it may be desirable for operational purposes to make use of intermediate results once a certain amount of data has been received. In this situation, the authorised processing must be allowed to complete so that the full set of results is obtained. Where there is any doubt regarding the compliance with an authorisation of activity to be undertaken by the request filter, the SPoC may be approached for confirmation.

9.15 The request filter performs the authorised processing of the communications data that has been disclosed to produce a results file. The only communications data that is processed is that disclosed by the communications providers for the purpose of the relevant authorisation. Only the results from the filter processing are released to the SPoC. An additional check may be used prior to release to confirm that the number of results are within specified limits.

Data management

9.16 The request filter will be operated on behalf of the Secretary of State by the Home Office. In practice the service will be provided by one or more third parties under contract.

9.17 The data owner for any authorised communications data disclosed to the request filter will be the designated senior officer at the authorising public authority. The data processor for all data disclosed to the request filter will be the Home Office (or another public authority designated by the Secretary of State by regulations). Once any data is disclosed to a public authority, that public authority is the data owner and processor for that disclosed data.

9.18 The communications data associated with an authorisation will be temporarily retained in the request filter until either the authorised processing is complete or, prior to that it ceases to be necessary to retain the data for the purpose concerned.

9.19 Those operating the request filter may periodically check with the relevant SPoC whether an authorisation remains valid if it has not been able to complete the processing. In any case, the relevant SPoC should notify the request filter immediately if the purpose of an authorisation is no longer valid so that any communications data associated with that authorisation is deleted and any outstanding or further data requests are cancelled.

9.20 Once the results have been released and the authorisation is complete, the disclosed communications data (including the results) are deleted from the request filter. Only audit and logging data is retained in the filter in accordance with requirements in the Act. This deletion is independent of CSP retention systems which will continue to hold the data for their normal retention period.

9.21 The request filter will only disclose communications data to the person identified in the relevant authorisation, or the designated senior officer concerned in accordance with section 66 of the Act.

9.22 The Secretary of State may in addition permit designated individuals to read, obtain or otherwise process data for the purposes of support, maintenance, oversight, operation or administration of the request filter.

9.23 The request filter will generate management and reporting information for a number of purposes including:

- Providing designated senior officers with information to inform decisions on the necessity and proportionality of authorisations;
- Support, maintenance, oversight, operation or administration of the arrangements; and
- The functions of the Investigatory Powers Commissioner.

9.24 This information may only be disclosed to:

- Designated senior officers for the purposes of determining the necessity and proportionality of an authorisation;
- Individuals designated by the Secretary of State for the purposes of support, maintenance, oversight, operation or administration of the request filter;
- The Investigatory Powers Commissioner for the purposes of the functions of the Commissioner; or
- When otherwise authorised by law.

9.25 Given the sensitivity of the data handled by the request filter, the Secretary of State must ensure that sufficient protections are in place to ensure the security of the system and protect against unauthorised and/or unlawful data retention, processing, access or disclosure. The filter will be operated under government security accreditation in accordance with government security policies and relevant standards. This will cover as a minimum:

- Protection of personal data disclosed by CSPs to the request filter in accordance with an authorisation;
- Controls, monitoring and audit of access to and use of the request filter;
- Restrictions regarding disclosure of results from the request filter;
- Provisions for deletion of material when no longer necessary or proportionate to retain it; and
- Those provisions outlined in chapter 11 regarding data protection.

9.26 Data disclosed to the public authority as a result of use of the request filter must be handled in accordance with the detail outlined in chapter 11.

Oversight and reporting

9.27 The request filter will be overseen by the Investigatory Powers Commissioner who will keep the use of the request filter by public authorities under review. This will form part of the Commissioner's broader audit, inspection and investigation regime for public authorities and their acquisition of communications data.

9.28 The Secretary of State must consult the Investigatory Powers Commissioner about the principles on the basis of which the request filter will be established, maintained or operated.

9.29 The Investigatory Powers Commissioner will receive an annual report regarding the functioning of the request filter during that year. The report will include details of verification and quality assurance activities, data deletion, security arrangements, and the operation and use of the arrangements. The Commissioner may use the information to inform its audit and inspection activities, and may conduct investigations into any specific issues arising from the report. As a result the Commissioner may require changes to be made to the use, operation, or design of the filtering arrangements.

9.30 The error reporting provisions detailed in Chapter 21 apply to the request filter. Should any significant processing errors occur which give rise to a contravention of any requirements in Part 3 of the Investigatory Powers Act, the fact must be reported to the Investigatory Powers Commissioner immediately. Where one technical system error occurs it could have multiple consequences. Such errors could, for example include the omission of, or incorrect matches in filtered results, or the release of results that exceed specified thresholds. For more detail see Chapter 21.

10 Maintenance of a technical capability

10.1 CSPs may be required under section 229 of the Act to provide a technical capability to give effect to a notice or authorisation under Part 3. The purpose of maintaining a technical capability is to ensure that, when a Part 3 notice or authorisation is in place, companies can give effect to it securely and quickly. In practice, these requirements will only be placed on companies that are required to give effect to notices or authorisations on a recurrent basis.

10.2 The Secretary of State may give a relevant CSP a "technical capability notice" imposing on the relevant operator obligations specified in the notice, and requiring the person to take all steps specified in the notice.

10.3 The obligations the Secretary of State considers reasonable to impose on CSPs are set out in regulations made by the Secretary of State and approved by Parliament, and may include (amongst others) the obligations set out in section 229(5) of the Act:

- Obligations to provide facilities or services of a specified description;
- Obligations relating to apparatus owned or operated by a relevant operator;
- Obligations relating to the removal of electronic protection applied, by or on behalf of the relevant operator on whom the obligation has been placed, to any data;
- Obligations relating to the security of any postal or telecommunications services provided by the relevant operator; and
- Obligations relating to the handling or disclosure of any material or data.

10.4 An obligation placed on a CSP to remove encryption only relates to electronic protections that the company has itself applied to the data, or where those protections have been placed on behalf of that CSP. The purpose of this obligation is to ensure that the data can be provided in intelligible form. References to protections applied on behalf of the CSP include circumstances where the CSP has contracted a third party to apply electronic protections to a telecommunications service offered by that CSP to its customers.

10.5 In the event that a number of CSPs are involved in the provision of a service, the obligation to provide a capability, and to remove encryption, will be placed on the CSP which has the technical capability to give effect to the notice and on whom it is reasonable practicable to impose these requirements.

10.6 While an obligation to remove encryption may only relate to protections applied by or on behalf of the company on whom the obligation is placed, there will also be circumstances where a CSP removes encryption from data for their own business reasons. Where this is the case a public authority will also require the CSP, where applicable and when served with an authorisation, to provide that data in an intelligible form.

Consultation with service providers

10.7 Before giving a notice, the Secretary of State must consult the CSP. In practice, consultation is likely to take place long before a notice is given. The Government will engage with companies who are likely to be subject to a notice in order to provide advice and guidance, and prepare them for the possibility of receiving a notice.

10.8 Should the giving of a notice to a CSP be deemed appropriate, the Government will take steps to consult the company formally before the notice is given. Should the company have concerns about the reasonableness, cost or technical feasibility of requirements to be set out in the notice, these should be raised during the consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process.

Matters to be considered by the Secretary of State

10.9 Following the conclusion of consultation with a communications service provider, the Secretary of State will decide whether to give a notice. This consideration should include all the aspects of the proposed notice. It is an essential means of ensuring that the notice is necessary and proportionate to what is sought to be achieved and that proper processes have been followed.

10.10 As part of the decision the Secretary of State must take into account, amongst other factors, the matters specified in section 231(3):

- The likely benefits of the notice – this may take into account projected as well as existing benefits;
- The likely number of users (if known) of any postal or telecommunications service to which the notice relates – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the technical capability notice;
- The technical feasibility of complying with the notice – taking into account any representations made by the communications service provider and giving specific consideration to any obligations in the notice to remove electronic protections (as described at section 231(4));
- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the company as part of the notice, such as those relating to security. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money; and
- Any other effect of the notice on the communications service provider – again taking into account any representations made by the company.

10.11 In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision. Section 2 of the Act requires the Secretary of State to have regard to the following when giving, varying or revoking a notice:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means,

- the public interest in the integrity and security of telecommunication systems and postal services, and

- any other aspects of the public interest in the protection of privacy.

10.12 The Secretary of State may impose an obligation only, after considering of the points above, if he or she considers that the notice is necessary, and that the conduct required is proportionate to what is sought to be achieved. The obligations set out in the notice must be reasonable, and the Secretary of State must ensure that communications service providers are capable of providing the necessary technical assistance.

10.13 Before the notice may be given, a Judicial Commissioner must approve the Secretary of State's decision to give a notice. In deciding whether to approve the Secretary of State's decision to give a relevant notice, a Judicial Commissioner must review the Secretary of State's conclusions regarding the necessity of the notice and the proportionality of the conduct required by the notice.

Giving a technical capability notice

10.14 Once a notice has been signed by the Secretary of State and the decision to give a notice has been approved by a Judicial Commissioner, arrangements will be made for this to be given to the communications service provider. During consultation, it will be agreed who within the company should receive the notice and how it should be issued (i.e. electronically or in hard copy). If no recipient is agreed, then the notice will be issued to a senior executive within the company.

10.15 Section 229(8) provides that obligations may be imposed on, and technical capability notices given to, a CSP located outside the UK and may require things to be done outside the UK. Where a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given to the CSP:

- 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; or

- At an address in the UK specified by the person.

10.16 As set out in section 229(7), the notice will specify the period within which the CSP must undertake the steps specified in the notice. It will often be the case that a notice will require the creation of dedicated systems. The time taken to design and construct such a system will be taken into account and, accordingly, different elements of the notice may take effect at different times.

10.17 A person to whom a technical capability notice is given is under a duty to comply with the notice. The duty to comply with a technical capability notice to give effect to communications data authorisations is enforceable against a person in the UK and a person outside the UK by civil proceedings by the Secretary of State.

Disclosure of technical capability notices

10.18 The Government does not publish or release identities of those subject to a technical capability notice as to do so may identify operational capabilities or harm the commercial interests of companies acting under a notice. Should criminals become aware of the capabilities of law enforcement, they may change their behaviours and communications service provider, making it more difficult to detect their activities of concern.

10.19 Any person to whom a technical capability notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence or contents of that notice to any person[52].

10.20 Section 231(8) provides for the CSP to disclose the existence and contents of a data retention notice with the permission of the Secretary of State. Such circumstances are likely to include disclosure:

- To a person (such as a system provider) who is working with the CSP to give effect to the notice;
- To relevant oversight bodies;
- To regulators in exceptional circumstances where information relating to a capability may be relevant to their enquiries;
- To other CSPs subject to a retention notice to facilitate consistent implementation of the obligations; and
- In other circumstances notified to and approved in advance by the Secretary of State.

Regular review

10.21 The Secretary of State must keep technical capability notices under review. This helps to ensure that the notice itself, or any of the requirements or restrictions imposed by it, remains necessary and proportionate.

10.22 It is recognised that, after a notice is given, the CSP will require time to take the steps outlined in the notice and develop the necessary capabilities. Until these capabilities are fully operational, it will be difficult to assess the benefits of a notice. As such, the first review should not take place until after these are in place.

10.23 A review of a technical capability notice will take place at least once every two years once capabilities are in place. However, the exact timing of the review is at the Secretary of State's discretion.

10.24 A review may be initiated earlier than scheduled for a number of reasons. These include:

[52] See section 231(8)

- A significant change in demands by law enforcement agencies that calls into question the necessity and proportionality of the notice as a whole, or any element of the notice;
- A significant change in CSP activities or services; or
- A significant refresh or update of CSP systems.

10.25 The process for reviewing a notice is similar to the process for giving a notice. The Government will consult the communications service provider as part of the review. Once this process is complete, the Secretary of State will consider whether the notice remains necessary and proportionate.

10.26 A review may recommend the continuation, variation or revocation of a notice. The relevant communications service provider and the operational agencies will be notified of the outcome of the review.

Variation of technical capability notices

10.27 The communications market is constantly evolving and CSPs subject to technical capability notices will often launch new services.

10.28 CSPs subject to a technical capability notice must notify the Government of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require the CSP to provide a technical capability on the new service.

10.29 Small changes, such as upgrades of systems which are already covered by the existing notice, can be agreed between the Government and CSP in question. However, significant changes will require a variation of the technical capability notice.

10.30 Section 232 of the Act provides that technical capability notices can be varied by the Secretary of State. There are a number of reasons why a notice might be varied. These include:

- a CSP launching new services;
- changing law enforcement demands and priorities;
- a recommendation following a review (see section above); or
- to amend or enhance the security requirements.

10.31 Where a CSP has changed name, for example as part of a rebranding exercise or due to a change of ownership, the Government, in consultation with the CSP, will need to consider whether the existing notice should be varied.

10.32 Before varying a notice, the Government will consult public authorities to understand the operational impact of any change to the notice, and the CSPs to understand the impact on them, including any technical implications. Once this consultation process is complete, the Secretary of State will consider whether it is necessary to vary the notice and whether the new requirements imposed by the notice as varied are proportionate to what is sought to be achieved by that conduct.

10.33 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraphs 10.9-10.12.

10.34 Once a variation has been agreed by the Secretary of State, arrangements will be made for the CSP to receive notification of this variation and details of the timeframe in which the variation needs to be enacted by the CSP. The time taken to implement these changes will be taken into account and, accordingly, different elements of the variation may take effect at different times.

Revocation of technical capability notices

10.35 A technical capability notice must be revoked (in whole or in part) if it is no longer necessary to require a CSP to provide a technical capability.

10.36 Circumstances where it may be appropriate to revoke a notice include where a CSP no longer operates or provides the services to which the notice relates, where operational requirements have changed, or where such requirements would no longer be necessary or proportionate.

10.37 The revocation of a technical capability notice does not prevent the Secretary of State issuing a new technical capability notice, covering the same, or different, services to the same CSP in the future should it be considered necessary and proportionate to do so.

11 General safeguards

11.1 This section relates to data protection requirements for data held by a public authority which was acquired under Part 3 of the Act.

11.2 Communications data acquired or obtained under the provisions of the Act may only be held for one or more of the statutory purposes for which the public authority can acquire communications data. Any data obtained through the Act, and all copies, extracts and summaries of it, must be handled and stored securely in accordance with the relative sensitivity of the data. Such data as is held should be adequate, relevant and not excessive in relation to the purpose.

11.3 In addition, the requirements of the DPA[53] and its data protection principles must be adhered to.

11.4 Communications data held by a public authority should be treated as information with a classification of OFFICIAL and a caveat of SENSITIVE, though it may be classified higher if appropriate[54]. The SENSITIVE caveat is for OFFICIAL information that is subject to 'need to know' controls so that only authorised personnel can have access to the material. This does not preclude, for example, the disclosure of material or the use of this material as evidence in open court when required. Rather, the classification and caveat of OFFICIAL - SENSITIVE makes clear that communications data must be treated with care, noting the impact on the rights to privacy and, where appropriate, freedom of expression of the subjects of interest and, depending on the data, possibly some of their communications contacts.

11.5 Communications data that is obtained directly as a consequence of the execution of an interception warrant must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 51 of the Act.

11.6 Communications data acquired under the Act must be held in a manner which provides the adequate level of protection for the relative sensitivity of the data and meets the data protection principles outlined in the DPA. Data must be effectively protected against unauthorised access to and use of that data, with particular consideration given to the principles of data security and integrity.

11.7 Access to communications data must be limited to the minimum number of trained individuals necessary for the authorised purposes. Individuals should be granted access only where it is required to carry out their function in relation to one of the purposes for which the public authority may acquire communications data.

---

[53] Guidance is available from www.justice.gov.uk/information-access-rights/data-protection *or* www.ico.org.uk.

[54] Details of government security classifications can be found at https://www.gov.uk/government/publications /government-security-classifications. Those who do not use these classifications should treat information in the appropriately equivalent manner under their data security rules.

11.8 A public authority may disclose communications data acquired under the Act only to the minimum extent necessary. The individual or organisation to which it is to be disclosed must require access for purposes consistent with those in the Act. On occasions where it is necessary for a public authority to disclose data to an overseas authority, the process outlined in paragraphs 11.29 – 11.33 should be followed.

11.9 When sharing data, the relevant public authority must be satisfied that the data will be adequately protected and that safeguards are in place to ensure this. All data shared must be afforded the same protections as it would receive at the public authority which originally acquired it. Appropriate limitations must be placed on the number of people to whom material is disclosed and the extent to which material is disclosed.

11.10 Data may only be held for as long as the relevant public authority is satisfied that it is still necessary for a statutory purpose. When it is no longer necessary or proportionate to hold such data, all relevant data must be destroyed. Data must be deleted such that it is impossible to access at the end of the period for which it is required.

11.11 Where it is necessary to process communications data acquired under the Act, public authorities must ensure that this is carried out in accordance with the DPA principles. This includes only processing such data where it is necessary, lawful and with appropriate safeguards. Public authorities must ensure that appropriate measures are in place to prevent unauthorised or unlawful processing and accidental loss or destruction of, or damage to, this data.

11.12 Where it is necessary to process communications data acquired under the Act together with data from other sources, the public authority must ensure that either it remains possible to identify the source of the data and apply security provisions accordingly or the resultant combined data is subject to the same or more stringent security provisions.

Disclosure of communications data and subject access rights

11.13 This section of the code provides guidance on the relationship between disclosure of communications data under the Act, CSPs' obligations to comply with a notice to disclose data, and individuals' right of access under section 7 of the DPA to personal data held about them.

11.14 The provisions regarding subject access requests[55] made under section 7 of the DPA apply notwithstanding the offence at section 79of the Act. However a CSP may rely on certain exemptions to the right of subject access under Part IV of the DPA[56].

[55] The Information Commissioner has produced a Subject Access Code of Practice to assist organisations adopt good practice when handling subject access requests, which is available at: ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf.

[56] There may be other bars to disclosure in other legislation, for example regarding impeding an investigation.

11.15 Section 28[57] of the DPA provides that data are always exempt from section 7 where such an exemption is required for the purposes of safeguarding national security.

11.16 Section 29 of the DPA provides that personal data processed for the purposes of the prevention and detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature are exempt from section 7 to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters.

11.17 The exemption to subject access rights possible under section 29 of the DPA does not automatically apply. In the event that a CSP receives a subject access request where the fact of a disclosure under the Act might itself be disclosed, the CSP concerned must carefully consider whether in the particular case disclosure of the fact of the authorisation would be likely to prejudice the prevention or detection of crime.

11.18 Where a CSP is uncertain whether disclosure of the fact of a notice would be likely to prejudice an investigation or operation, it should approach the SPoC of the public authority which gave the notice – and do so in good time to respond to the subject access request. The SPoC can make enquiries within the public authority to determine whether disclosure of the fact of the notice would likely be prejudicial to the matters in section 29. As paragraph 4.71 requires a notice to set out whether a CSP may inform the subject a request for their data has been made, such circumstances would be limited[58].

11.19 Where a CSP withholds a piece of information in reliance on the exemption in section 28 or 29 of the DPA, it is not obliged to inform an individual that any information has been withheld. It can simply leave out that piece of information and make no reference to it when responding to the individual who has made the subject access request.

11.20 A CSP should not provide information in response to a subject access request where doing so would be an offence under section 79 of the Act.

11.21 CSPs should keep a record of the steps they have taken in determining whether disclosure of the fact of a notice would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police. Under section 42 of the DPA an individual may request that the Information Commissioner assesses whether a subject access request has been handled in compliance with the DPA.

---

[57] Section 28(2) of the DPA makes clear that a certificate from a Minister of the Crown is conclusive evidence, though this can be challenged through appeal to a Tribunal.

[58] The SPoC must provide a response which will enable the CSP to comply with its obligations to respond to the subject access request within 40 days at the latest.

Acquisition of communication data on behalf of overseas authorities

11.22 While the majority of public authorities which obtain communications data under the Act have no need to disclose that data to any authority outside the United Kingdom, there can be occasions when it is necessary, appropriate and lawful to do so in matters of international co-operation.

11.23 There are two methods by which communications data, whether obtained under the Act or not, can be acquired and disclosed to overseas public authorities[59]:

- Judicial co-operation; or
- Non-judicial co-operation.

Neither method compels United Kingdom public authorities to disclose data to overseas authorities. Data can only be disclosed when a United Kingdom public authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled.

Judicial co-operation

11.24 A central authority in the United Kingdom may receive a request for mutual legal assistance (MLA) which includes an application for communications data from an overseas court exercising criminal jurisdiction, an overseas prosecuting authority, or any other overseas authority that appears to have a function of making requests for MLA. This MLA request must be made in connection with criminal proceedings or a criminal investigation being carried on outside the United Kingdom, and the application for communications data included must be capable of satisfying the requirements of Part 3 of the Act.

11.25 If such an MLA request is accepted by the central authority, it will be referred for consideration by the appropriate public authority in the UK. The application may then be considered and, if appropriate, executed by that public authority under section 58 of the Act and in line with the guidance in this code of practice.

11.26 In order for a notice or authorisation to be granted, the United Kingdom public authority must be satisfied that the application meets the same criteria of necessity and proportionality as required for a domestic application.

Non-judicial co-operation

11.27 Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries. These can include applications for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such an application, the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Part 3 of the Act.

11.28 The United Kingdom public authority must be satisfied that the application complies with United Kingdom obligations under human rights legislation. The necessity and proportionality of each case must be considered before the authority processes the authorisation or notice.

---

[59] This includes public authorities within the Crown Dependencies and the British Overseas Territories.

Disclosure of communications data to overseas authorities

11.29 Where a United Kingdom public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring the data to that authority, it must consider whether the data will be adequately protected outside the United Kingdom and what safeguards may be needed to ensure that. Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

11.30 If the proposed transfer of data is to an authority within the European Union, that authority will be bound by European data protection legislation and its national data protection legislation. Any data disclosed will be protected there without need for additional safeguards.

11.31 If the proposed transfer is to an authority outside of the European Union and the European Economic Area (Iceland, Liechtenstein and Norway), then it must not be disclosed unless the overseas authority can ensure an adequate level of data protection. The European Commission has determined that certain countries, for example Switzerland, have laws providing an adequate level of protection where data can be transferred without need for further safeguards[60].

11.32 In all other circumstances, the United Kingdom public authority must decide in each case, before transferring any data overseas, whether the data will be adequately protected there. The Information Commissioner has published guidance on sending personal data outside the European Economic Area in compliance with the Eighth Data Protection Principle, and, if necessary, his office can provide guidance.

11.33 The DPA recognises that it will not always be possible to ensure adequate data protection in countries outside of the European Union and the European Economic Area, and there are exemptions to the principle, for example if the transfer of data is necessary for reasons of 'substantial public interest'[61]. There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data. That is a decision that can only be taken by the public authority holding the data on a case by case basis.

[60] The relevant Commission webpage is at: http://ec.europa.eu/justice/data-protection//international-transfers/adequacy/index_en.htm.

[61] Paragraph 4, Schedule 4, DPA.

12 Compliance and offences

12.1 The Act places a requirement on CSPs to comply with a requirement imposed on them by a notice under Part 3 of the Act, but are not required to take any steps which it is not reasonably practicable for them to take. Where a technical capability notice is in place an operator will be considered as having put in place the capabilities specified in that notice when consideration is given to their compliance with a notice.

12.2 What is reasonably practicable will be considered on a case-by-case basis, taking into account the individual circumstances of the relevant CSP. Such consideration is likely to cover a number of factors including, but not limited to, the technical feasibility and likely cost of complying with the notice.

12.3 Where a technical capability notice is in place an operator will be considered as having put in place the capabilities specified in that notice when consideration is given to their compliance with the obligation.

12.4 Section 82 of the Act provides that where such 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 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 notifying the person by such other means as the authorised officer considers appropriate (which may include notifying the person orally).

12.5 When considering whether a notice given to a person outside the UK is reasonably practicable, section 82(4)(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 proceed with civil proceedings.

12.6 The duty of compliance in relation to Part 3 of the Act is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988 or for any other statutory relief.

Offences

12.7 The Act creates two offences which are relevant to the acquisition and disclosure of communications data.

Acquisition Offence

12.8 Under section 11 of the Act, it is an offence for a person in a public authority knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority.

12.9 The creation of the offence of unlawfully obtaining communications data reflects the sensitivity of communications data and the need for careful consideration in authorisation of its acquisition. The roles and responsibilities laid down for the senior responsible officer, designated senior officer and SPoC are designed to prevent the 'knowing or reckless' acquisition of communications by a public authority where it does not hold a lawful authorisation. Proper adherence to the requirements of the Act and this code, including following the procedures identified in chapter 4, will ensure no offence is committed.

12.10 It is a defence if the person who obtained the communications data can show that action was taken in the reasonable belief that they had, in law, the right to obtain that data.

12.11 This offence is not designed to capture errors on behalf of the public authority but rather, for example, instances where a person in a public authority failed to take account of obvious risk or where a person in a public authority deliberately fails to obtain an authorisation or obtains communications data from a CSP despite the fact that they could not have genuinely believed that an authorisation would be in place.

12.12 In particular, it is not an offence to obtain communications data where it is made publicly or commercially available by the CSP or otherwise where the CSP freely consents to its disclosure. In such circumstances the consent of the operator provides the lawful authority for the obtaining of the data.

Disclosure offence

12.13 Under section 79, it is an offence for a telecommunications operator to disclose without reasonable excuse the existence of a request for communications data by a public authority under the Act.

12.14 The offence of unauthorised disclosure occurs when any CSP, or employee of a CSP, reveals the existence of either a requirement to disclose communications data about a particular person to that person.

12.15 It is a reasonable defence for a CSP to disclose such information when the public authority making the request for data gives permission to do so. A public authority must indicate in the authorisation for obtaining of communications data whether it gives permission to the CSP to disclose the request for communications data. If permission is given, the public authority must specify to the CSP the circumstances under which disclosure may take place.

12.16 When considering whether or not to give permission to disclose the existence of a specific request for communications data, the public authority must consider the specific circumstances of the operation or investigation to which the request refers. Where no circumstances preventing disclosure are identified, permission should be given.

12.17 Circumstances which may prevent permission being given may include, but are not limited to:

- The interests of other public authorities in the operation or investigation;
- Any potential negative impact on future operational or investigative capability; and
- The undermining of the purposes outlined in section 58(7) of the Act.

12.18 Circumstances in which it may be appropriate to give permission to disclose the existence of a specific request for communications data may include where communications data is requested to assist in the investigation of a crime of which the subject of the request is the victim – for example where a person's phone has been stolen and the police seek communications data in order to locate the phone.

12.19 It would not be a reasonable defence for a CSP to disclose such information in the interests of transparency to its customers without the permission of the relevant public authority.

Part 3

Communications Data Retention

13 General extent of powers

Necessity and proportionality

13.1 Section 84(1) of the Act gives the Secretary of State the power to issue a data retention notice to a CSP, requiring them to retain relevant communications data, if it is considered necessary and proportionate for data to be retained for one or more of the purposes in section 58(7) of the Act. These are:

- In the interests of national security;
- For the purpose of preventing or detecting crime[62] or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- In the interests of public safety;
- For the purpose of protecting public health;
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- For the purpose, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- To assist investigations into alleged miscarriages of justice;
- For the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime (such as a natural disaster or an accident);
- In relation to a person who has died or is unable to identify himself, for the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for his death or condition; and
- For the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.

13.2 Section 2 of the Act requires the Secretary of State to have regard to the following when giving, varying or revoking a notice:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means,
- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.

---

62 Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed. See section 239(1) of the Act.

13.3 Data retained for the purposes set out above can only be accessed by public authorities for those purposes under Part 3 of the Act, or other appropriate statutory regime, where it is necessary and proportionate to do so. The consideration of necessity and proportionality involves balancing the extent of the interference with an individual's right to respect for their private life and, where relevant, with freedom of expression, against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest. Further information on this can be found in chapter 3 of this code.

14 Giving of data retention notices

Process for giving a data retention notice

14.1 The Home Office and key operational agencies (including law enforcement agencies and security and intelligence agencies) maintain governance arrangements in order to identify operational requirements, including the potential requirement to issue a data retention notice.

14.2 Once a potential requirement is identified, the Home Office will consult the relevant CSP(s) and, if appropriate, the Secretary of State will consider giving a notice.

Criteria for issuing a data retention notice

14.3 When considering whether to issue a notice a number of factors are taken into account. These include, but are not limited, to:

- The size of a CSP – a CSP with a larger customer base is more likely to receive a data retention notice;
- The speed of growth of a CSP – small CSPs with rapid prospective growth may receive notices in anticipation of future law enforcement requirements;
- The number of requests a CSP receives annually for communications data – this, and the CSPs ability to meet the volume of requests they receive, will be a key determinant of whether there is benefit in serving a notice on a CSP (noting that the giving of a notice may increase the number of requests received by a CSP);
- Whether a CSP operates a niche service – a CSP which is the sole or key provider of a type of service may receive a notice regardless of the size of the company; or
- Whether a CSP operates in a specific geographical area – a CSP which is a key provider of services in a limited geographical area is more likely to receive a notice.

14.4 Ultimately, however, a notice can only be given where the Secretary of State, having taken into account relevant information, considers it necessary and proportionate to do so.

14.5 The timescale for such processes will depend on operational need but will always follow the same steps to ensure that the Secretary of State is making an informed decision, based on the relevant information.

14.6 Where a company uses the physical network (this includes the network bandwidth and phone lines) belonging to another in order to provide their services to the public, a retention notice can be imposed on whichever company holds the relevant communications data (which will depend on how they design and operate their systems). The Home Office will work with providers to ensure that public authorities are aware of which company is best placed to respond to requests for the data.

14.7 Where two companies under a retention notice hold similar or identical data or are capable of doing so the Home Office will agree an approach with the providers concerned to ensure that the relevant data is not retained more than once.

Criteria for giving a notice to categories of providers

14.8 There may be circumstances where there are a number of CSPs providing similar services in a specific limited area. An example of this could be Wi-Fi providers in a particular location.

14.9 It is possible that the Secretary of State could place the same obligations on all such CSPs through one notice, but only if it was considered necessary and proportionate to do so.

14.10 While this may be appropriate for a relatively small number of providers providing the same or a similar service, this provision cannot be used to place blanket requirements across a large number of companies operating a service or companies providing a range of different services, not least because the requirements in a notice need to reflect the particular nature of each business.

Consultation with service providers

14.11 Before giving a notice to a company the Secretary of State must take reasonable steps to consult any CSP(s) which will be subject to the notice.

14.12 In practice, consultation is likely to take place long before giving a notice to a company. The Home Office will engage with companies who may possibly be subject to a notice in the future to provide advice and guidance and prepare them for the possibility of receiving a notice should it be considered necessary and proportionate to do so.

14.13 Should the giving of a notice to a CSP be deemed appropriate, the Home Office will take steps formally to consult the company before giving a notice, in order to ensure that it accurately reflects the services and data types processed by that CSP and to ensure that the CSP understands the obligations being placed on it, including those in relation to the audit functions of the Information Commissioner.

14.14 Should a CSP have concerns about whether the requirements of a notice are appropriate or technically feasible, these should be raised during this consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process. Should a CSP continue to have concerns in respect of the feasibility of a notice once given they may refer the notice for review (see chapter 20).

14.15 Should it be considered appropriate to place the same obligations on a number of companies through one notice, the Home Office will take steps to consult all CSPs who would or could be affected by the notice. However, it is recognised that there may be cases where this will not be possible, for example where a new CSP enters the market after a notice is given and therefore will not have been formally consulted. In such circumstances the Secretary of State must take reasonable steps to consult any relevant CSP(s) which enter the market after such a notice is issued.

Matters to be considered by the Secretary of State

14.16 Following the conclusion of consultation with CSPs, the Secretary of State will consider whether to give a data retention notice. This consideration should include all the aspects of the proposed data retention notice. It is an essential means of ensuring that the data retention notice is justified and that proper processes have been followed.

14.17 As part of the decision the Secretary of State must take into account a number of factors:

- The likely benefits of the notice – the extent to which the data to be retained may be of use to public authorities. This may take into account projected as well as existing benefits;
- The likely number of users of the services to be covered by the notice – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the data being retained;
- The technical feasibility of complying with the notice – taking into account any representations made by the CSP(s);
- The likely cost of complying with the notice – this will include the costs of both the retention, and any other requirements and restrictions placed on CSPs, such as ensuring the security of the retained data. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money[63]; and
- Any other impact of the notice on the CSP – again taking into account any representations made by the CSP(s).

14.18 The Secretary of State will also consider the contents of the proposed notice, including the data to be retained and the period or periods for which that data is to be retained up to a maximum of 12 months from the giving of the notice[64].

14.19 In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision.

14.20 If the Secretary of State agrees with the recommendation to give a notice, they will then sign the notice.

Once a notice has been signed

14.21 Once a notice has been signed by the Secretary of State, arrangements will be made for this to be given to a CSP. During consultation with the CSP, it will be agreed who in the company should receive the notice and how it should be issued (i.e. electronically or in hard copy). If no recipient is agreed, then the notice will be issued to a senior executive within the company.

14.22 A data retention notice comes into force from the point it is given to the CSP, unless otherwise specified in the notice.

---

63 See paragraph 10.10 for details of the matters the Secretary of State will consider before issuing a data retention notice.

64 See paragraphs 14.30-14.37 for further information on retention periods.

14.23 It will often be the case that dedicated systems will be constructed within a CSP for the retention of communications data, and the time taken to design and construct such a system will be taken into account. Accordingly, different elements of the notice may take effect at different times.

14.24 Once a notice has been given to a CSP, a copy of the notice and any other relevant information will be sent to the Information Commissioner, who is responsible for auditing the security, integrity and destruction of retained data (see chapter 22 for further details).

The content of a data retention notice

14.25 A notice will set out:

- The CSP(s) to which it relates – where a company owns a number of subsidiary companies that operate under different trading names, the notice might additionally list these details for the sake of clarity;
- Which services data is to be retained for – it may not be necessary and proportionate to retain data in relation to all communication services provided by a company;
- The data to be retained and the period for which it is retained – these will relate to the categories of data listed as 'relevant communications data' in section 84(10) of the Act and will make clear whether certain categories of data should be retained for less than 12 months; and
- Any additional requirements or restrictions in relation to the retention of the data – this may include requirements in relation to the security, integrity and destruction of retained data and the audit of the CSPs compliance with these requirements by the Information Commissioner.

14.26 A notice will not necessarily represent the full range of services and data types which a CSP could retain. This does not mean that additional data types or services could not be included in a future version of the notice, should a pressing operational requirement arise, provided that it would be necessary and proportionate to do so (see chapter 15 for further details).

14.27 Requirements or restrictions in relation to the retention of the data may include:

- A requirement to take such steps as are necessary to ensure that data which is generated and processed by the CSP (including transitory information in the core systems) is made available to be retained; or
- A requirement to process the data to ensure that multiple items of data from a single or multiple CSP systems can be stored in a single clear record where appropriate to do so. This will ensure the volume of data retained is limited to that which is truly necessary.

Generation & processing of data

14.28 A retention notice may include requirements in relation to the retention of data. Such requirements may include:

- A requirement to retain data in such a way that it can be transmitted efficiently and effectively in response to requests (including linking events to user accounts);
- A requirement to take such steps as are necessary to ensure that data which is generated and processed by the CSP but not collected for business purposes is made available to be retained (this could include extracting or generating data from transitory information in the core network components or from network traffic);
- A requirement to process the data to ensure that multiple items of data from a single or multiple CSP systems can be stored in a single clear record where appropriate to do so; and
- A requirement to filter the data to remove records that are not of interest, including duplicate events or where aggregated records or summaries have been created;

14.29 Aggregation, summarisation and filtering of data will ensure the volume of data retained is limited to that which is truly necessary.

Retention period

14.30 Data retained under the Act may be retained for a maximum of 12 months.

14.31 A notice will only require data to be retained for as long as is considered necessary and proportionate, up to that maximum period. If, once a data retention notice is given, further evidence demonstrates that a retention period specified in the notice is no longer appropriate, the Secretary of State will set a different retention period, up to a maximum of 12 months, ensuring the period reflects what is necessary and proportionate.

14.32 A data retention notice may cover data already in existence at the point at which a notice is given or it may require the generation of data.

14.33 The starting point for the retention period for data in existence at the point of the notice is determined by the type of data.

14.34 The retention period for a specific communication commences on the day of the communication concerned. Some internet communications, such as broadband sessions, may remain active for days, or even months. In such cases the retention period commences on the day on which the communication ends.

14.35 For data held by a CSP about an entity to whom a service is provided the retention period commences on the day on which the entity concerned ceases to be connected to the service or if the data is changed. For example previous addresses for a customer may only be retained for 12 months after the CSP changes the data in their systems, irrespective of whether the customer remains with the service.

14.36 For all other communications data held by a CSP, including where data is required to be generated, then the retention period will start from the moment the data comes into existence.

14.37 Sometimes a CSP may already retain data for 12 months or more for business purposes. Such data may still be subject to a retention notice to ensure that the

data is available with the maximum 12 month period in case the business need for the data changes and the CSP decides to delete the data.

15 Review, variation and revocation of retention notices

Review

15.1 The Secretary of State must keep notices under review. This helps to ensure that a notice itself, or the retention of categories of data specified in a notice, remains necessary and proportionate.

15.2 It is recognised that, after a notice is given, a CSP is likely to require time to put the necessary capabilities in place to meet their obligations. As such, the first review should not take place until after these capabilities have been put in place. Without these capabilities being fully operational, it will not generally be possible to assess the benefits of a notice.

15.3 Reviews will take place at least once every two years once capabilities are in place. However, the exact timing of the review is at the Secretary of State's discretion.

15.4 A review may be initiated earlier than scheduled for a number of reasons. These include:

- A significant change in demands by law enforcement agencies that calls into question the necessity and proportionality of the notice as a whole, or a subset of data being retained under a notice;
- A significant change in CSP activities or services; or
- A significant refresh or update of CSP systems.

15.5 The process for reviewing a notice is similar to the process for giving a notice, with the Home Office consulting operational agencies and CSPs as part of the review. In addition the Home Office will consult the Information Commissioner as part of the review.

15.6 The review will also take into account the number of law enforcement requests made and the age of the data obtained. An absence – or low volume – of law enforcement requests will not necessarily mean that it is no longer necessary and proportionate to maintain a data retention notice.

15.7 Once this process is complete, the Secretary of State will consider whether the notice remains necessary and proportionate.

15.8 A review may recommend the continuation, variation or revocation of a notice. Details of the variation of and revocation of data retention notices follow below.

15.9 The relevant CSP, the operational agencies and the Information Commissioner will be notified of the outcome of the review.

Variation

15.10 The communications market is constantly evolving and CSPs subject to data retention notices will often launch new services or generate new data that law enforcement may require.

15.11 CSPs subject to a data retention notice must notify the Home Office of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require data generated or processed in the course of providing those services to be retained.

15.12 Small changes, such as upgrades of systems or changes to data which are already covered by the existing notice, can be agreed between the Home Office and CSP in question. However, significant changes will require a variation of the data retention notice.

15.13 Section 89 of the Act provides that data retention notices can be varied by the Secretary of State. There are a number of reasons why a notice might be varied. These include:

- a CSP launching new services or generating new categories of communications data which may be of interest to law enforcement;
- changing law enforcement demands and priorities;
- a recommendation following a review (see review section above); or
- to amend or enhance the security requirements – for example following an audit of the security, integrity and destruction of retained data by the Information Commissioner.

15.14 Where a company has changed names, for example as part of a rebranding exercise or due to a change of ownership, the Home Office and the company will need to consider whether the existing notice is sufficient.

15.15 The process for varying a notice is similar to the process for giving a notice. The Home Office will consult operational agencies, to understand the operational impact of any change to the notice, and CSPs to understand the impact on them, including any technical implications. Once this consultation is complete, the Secretary of State will consider whether to vary the notice.

15.16 Further detail on the process for consultation with CSPs and consideration by the Secretary of State can be found in chapter 14.

15.17 Once a variation has been agreed by the Secretary of State, arrangements will be made for this to be given to a CSP. As with a data retention notice, a variation of a notice comes into force from the point it is given unless otherwise specified in the notice and different elements of the variation may take effect at different times.

15.18 Once a variation has been given to a CSP a copy will be sent to the Information Commissioner.

15.19 A data retention notice may be varied to reduce, or extend, the period for which data can be retained. No retention notice, or such variation, can result in data being retained for longer than 12 months.

Revocation

15.20 A data retention notice must be revoked (in whole or in part) if it is no longer necessary to require a CSP to retain communications data, or certain types of communications data.

15.21 Circumstances where it may be appropriate to revoke a notice include where a CSP no longer operates or provides the services to which the notice relates, where operational requirements no longer include the data covered by the notice, or where such requirements would no longer be necessary or proportionate.

15.22 The revocation of a data retention notice does not prevent the Secretary of State issuing a new data retention notice, covering the same, or different, data and services, to the same CSP in the future should it be considered necessary and proportionate to do so.

15.23 Once notice of revocation has been given to a CSP a copy will be sent to the Information Commissioner.

16 Security, integrity and destruction of retained data

16.1 All data retained under the Act is subject to a range of safeguards in order to ensure effective protection of the data against the risk of abuse and any unlawful access to and use of that data. Section 87 of the Act requires CSPs under a notice to take steps to ensure that the data is adequately protected while it is being retained. These requirements relate to three broad areas – data security, data integrity and destruction of data.

16.2 Further detail on the security arrangements to be put in place by CSPs may be included in the data retention notice given to a CSP which, in accordance with section 84(7)(d), must specify any other requirements or restriction in relation to the retention of data.

16.3 In most cases data retained under a notice is stored in dedicated data retention and disclosure systems, which are securely separated by technical security measures (e.g. a firewall) from a CSPs business systems. Where data is retained by CSPs for business purposes for some, but not all, of the period specified in the notice, the data retention and disclosure system may hold a duplicate of that business data so that it can be accessed efficiently and effectively[65].

16.4 However, in some cases it will not be practical to create a duplicate of that data and CSPs will retain information in business or shared systems.

16.5 The scope of the security controls defined within this section apply to all dedicated IT systems that are used to retain or disclose communications data, and any other dedicated systems which are used to access, support or manage dedicated retention and disclosure systems. It also applies to all CSP (or third party) operational and support staff who have access to such systems. Additional security considerations may be required to enable systems for the disclosure of communications data to connect securely to acquisition systems in public authorities.

16.6 Where data is retained in business or shared systems, or where business systems are used to access, support or manage retention and disclosure systems, these will be subject to specific security controls and safeguards, similar to those defined within this section, where appropriate and as agreed with the Home Office.

65 In accordance with section 84(8)(a).

Data security

16.7 The specific data security measures required by a CSP to protect retained data will depend on a number of factors including, but not limited to, the volume of data being retained, the number of customers whose data is being retained and the nature of the retained data.

16.8 When setting security standards consideration must also be given to the threat to the data.

16.9 The security put in place at a CSP will comprise four key areas:

- Physical security e.g. buildings, server cages, CCTV;
- Technical security e.g. firewalls and anti-virus software;
- Personnel security e.g. staff security clearances and training; and
- Procedural security e.g. processes and controls.

16.10 As each of these broad areas is complementary, the balance between these may vary e.g. a CSP with slightly lower personnel security is likely to have stricter technical and procedural controls. The specific security arrangements in place will be agreed in confidence between the Home Office and relevant CSPs and shared with the Information Commissioner for his functions under this code.

16.11 As the level of data security is based on a number of factors and is a balance of four broad areas, there is no single minimum security standard. However, all CSPs retaining data will be required to follow the key principles of data security set out in paragraphs 16.18 to 16.41. It is open to a CSP to put in place alternative controls or mitigations which provide assurance of the security of the data where agreed with the Home Office.

16.12 The Home Office will provide security advice and guidance to all CSPs who are retaining data and this will be provided to the Information Commissioner for the conduct of his functions under this code.

Data integrity

16.13 Data integrity, as required by section 86(1)(a), relates to a need to ensure that no inaccuracies are introduced to data when it is retained under the Act and that the data is not varied[66].

16.14 When relevant communications data is retained under the Act, it should be a faithful reproduction of the relevant business data and it should remain a faithful reproduction throughout any further processing that may occur during the period of its retention. A record of the business purpose for which the data is generated may be retained to assist law enforcement to understand the underlying quality and completeness of the business data which has then been retained. For example, data generated to assist a CSP in understanding network loading may be less accurate than data used to bill customers.

---

66 This includes at the point at which it is placed into a data retention and disclosure system and during the period of its retention.

16.15 There should be no errors introduced in retaining the data, for example in the process of copying the data to a retained data store or in searching and disclosing data, that lead to discrepancies between the business and retention sets of data.

16.16 Once the data has been retained, technical security controls shall be implemented to mitigate modification of the data, and to audit any attempt to modify the data, until such time that it is deleted in accordance with section 87(2) of the Act.

16.17 The audit capability of the data retention system shall be used to provide assurance that no unauthorised changes have been made to the retained data.

Principles of data security, integrity and destruction

Legal and regulatory compliance

16.18 All data retention systems and practices must be compliant with relevant legislation. As well as the Act, this includes, but is not limited to, the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003, which set out key controls in relation to the storage, use and transfer of personal data.

16.19 All systems and practices must also comply with any security policies and standards in place in relation to the retention of communications data. This may include any policies and standards issued by the Home Office, and any instruction or recommendation made by the Information Commissioner such as his published guidance on security. These further requirements are unlikely to be publicly available as they may contain specific details of security infrastructure or practices, disclosure of which could create additional security risks.

Information security policy & risk management

16.20 Each CSP must develop a security policy document. The policy document should describe the internal security organisation, the governance and authorisation processes, access controls, necessary training, the allocation of security responsibilities and policies relating to the integrity and destruction of data. Each CSP must also develop security operating procedures, including clear desk and screen policies for all systems. A CSP can determine whether this forms part of or is additional to wider company policies.

16.21 The security policy document and security operating procedures should be reviewed regularly to ensure they remain appropriate to the nature of the business, the data retained and the threats to data security.

16.22 Each CSP must identify, assess and treat all information security risks, including those which relate to arrangements with external parties.

Human Resources security

16.23 CSPs must clearly identify roles and responsibilities of staff, ensuring that roles are appropriately segregated to ensure staff only have access to the information necessary to complete their role. Access rights and permissions assigned to users must be revoked on termination of their employment. Such rights and permissions must be reviewed and, if appropriate, amended or revoked when staff move roles within the organisation.

16.24 Staff with access to the data retention or disclosure systems should be subject to an appropriate level of security screening. The Government sponsors and manages security clearance for certain staff working within CSPs. CSPs must ensure that these staff have undergone relevant security training and have access to security awareness information.

Maintenance of physical security

16.25 Data retention and disclosure systems should have appropriate security controls in place. Access to the locations where the systems are both operated and hosted must be controlled such that access is limited to those with the relevant security clearance and permissions.

16.26 Equipment used to retain data must be sanitised and securely disposed of at the end of its life (see the section on destruction of data beginning at paragraph 16.42).

Operations management

16.27 Data retention and disclosure systems should be subject to a documented change management process, including changes to third party suppliers, to ensure that no changes are made to systems without assessing the impact on the security of retained data.

16.28 CSPs must also put in place a patching policy to ensure that regular patches and updates are applied to any data retention and disclosure system as appropriate. Such patches and updates will include anti-virus, operating systems, application and firmware. The patching policy, including the timescale in which patches must be applied, must be agreed with the Home Office.

16.29 CSPs should ensure that, where encryption is in place in data retention and disclosure systems, any encryption keys are subject to appropriate controls, in accordance with the security policy.

16.30 In order to maintain the integrity of internal data processing CSPs must ensure that data being processed is validated against agreed criteria.

16.31 Network infrastructure, services and system documentation must be secured and managed and an inventory of all assets should be maintained together with a clear identification of their value and ownership. All assets must be clearly labelled.

16.32 CSPs should also ensure that removable and storage media (including the hard drives used to store retained data) are managed in accordance with the security policy, especially when in transit.

16.33 The data retention and disclosure system, and its use, should be monitored and all audit logs compiled, secured and reviewed by the CSP security manager at appropriate intervals. These should be made available for inspection by the Home Office as required.

16.34 CSPs should ensure that systems are resilient to failure and data loss by creating regular back-ups of the data.

16.35 Technical vulnerabilities must be identified and assessed through an independent IT Health Check which must be conducted annually. The scope of the Health Check must be agreed with the Home Office.

Access controls

16.36 CSPs must ensure that registration and access rights, passwords and privileges for access to dedicated data retention and disclosure systems are managed in accordance with their security policy. They must also ensure that users understand and formally acknowledge their security responsibilities.

16.37 Access to operating systems must be locked down to an appropriate standard and any mobile computing (i.e. offsite access to CSP systems from non-secure locations) must be subject to appropriate policies and procedures if permitted. Accordingly any remote access for diagnostic, configuration and support purposes must be controlled.

16.38 Access should be provided to relevant oversight bodies where necessary for them to carry out their functions.

Management of incidents

16.39 CSPs must put in place clear incident management processes and procedures, including an escalation path to raise issues to senior management and the Home Office. Any breaches under relevant legislation, such as the Act or the Privacy and Electronic Communications Regulations 2003, should be notified in accordance with those provisions.

16.40 Measures should be implemented to prevent unauthorised disclosure or processing of data. Any suspected or actual unauthorised disclosure or processing of data or information must be reported as set out above.

16.41 System managers must ensure that data retention and disclosure systems enable the collection of evidence (e.g. audit records) to support investigation into any breach of security.

Additional requirements relating to the destruction of data

16.42 Section 87(2) makes clear that retained data must be destroyed[67] such that it is impossible to access at the end of the period for which it is required to be retained, unless its retention is otherwise authorised by law. A system must be set up such that it is verifiable that data is deleted and inaccessible at the end of the retention period. Deletions must take place at intervals no greater than monthly.

16.43 Where the physical, personnel and procedural security measures are assessed by the Home Office, or Information Commissioner, to be sufficient to prevent unauthorised physical access to the data retention and disclosure system, then data should be deleted in such a way that protects against data recovery using non-invasive attacks (i.e. attempts to retrieve data without additional assistance from physical equipment).

[67] Section 239(1) defines 'destroy' for the purposes of the Act to mean 'delete the data in such a way as to make access to the data impossible.'

16.44 Where the implemented security measures are assessed by the Home Office, or Information Commissioner, to be insufficient to protect the data retention and disclosure system against physical access by unauthorised personnel, then additional requirements for the secure destruction of retained data should be agreed with the Home Office and Information Commissioner on a case-by-case basis.

Additional requirements relating to the disposal of systems

16.45 The legal requirement to ensure deleted data is impossible to access must be taken into account when disposing of any system, or component of a system, which reaches the end of its service life.

16.46 If the equipment is to be re-used it must be securely sanitised by means of overwriting using a Home Office approved product. If the equipment is not to be re-used immediately, it must be securely stored in such a way that it may only be re-used or disposed of appropriately.

16.47 If the equipment is to be finally disposed of, it must be securely sanitised by means of physical destruction by a Home Office approved supplier.

16.48 Sanitisation or destruction of data must include retained data copied for back-up and recovery, and anything else that stores duplicate data within the CSP system, unless retention of the data is otherwise authorised by law.

17 Disclosure and use of data

Disclosure of data

17.1 As per section 87 of the Act, a CSP must put in place adequate security systems (including technical and organisational measures) governing access to retained communications data in order to protect against any unlawful disclosure.

17.2 Section 84(8)(a) of the Act also requires CSPs to retain data in such a way that it can be transmitted efficiently and effectively in response to requests for communications data. The Home Office will work with CSPs to ensure that the necessary secure auditable systems are in place to enable this disclosure.

17.3 The provisions on disclosure of retained data are intended to cover disclosure of communications data in response to requests made under Part 3 of the Act. However, there may be other circumstances in which CSPs may lawfully disclose retained communications data. Such circumstances could include:

- If an emergency service requests data in relation to an emergency call (chapter 8);
- Requests for personal data held by a company via a subject access request under the Data Protection Act 1998[68];
- Where a CSP proactively discloses communications data to relevant public authorities or regulatory bodies such as in cases of suspected criminality.

Use of data by communications service providers

17.4 If data is held subject to a notice and would not otherwise be held by the CSP for business purposes, it should be adequately safeguarded to ensure that it can only be accessed for lawful purposes. If data is not also being retained for existing business purposes it cannot be used by CSPs for business purposes, for example marketing, if such a requirement is subsequently identified.

[68] Section 27(5) of the Data Protection Act 1998 states that 'the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information.' There may be other exemptions from subject access rights in specific circumstances such as where providing access is likely to prejudice crime prevention purposes.

18 Compliance

18.1 The Act places a requirement on CSPs to take all such steps for complying with any duty imposed on them under Part 4 of the Act. The duty of compliance in relation to Part 4 of the Act is enforceable in relation to conduct or a person in the UK by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988 or for any other statutory relief.

18.2 That duty can only be enforced against a person who the authorities consider may be able to provide the assistance required by the notice.

Disclosure of a retention notice

18.3 The Home Office does not publish or release identities of CSPs subject to a data retention notice as to do so may identify operational capabilities or harm the commercial interests of CSPs under a notice. This is because if criminals are aware of the capabilities of law enforcement then they may change their communications service provider accordingly.

18.4 Section 90(2) of the Act prohibits a CSP or an employee of the CSP disclosing the existence of a retention notice or the content of the retention notice to any person. That duty is enforceable by civil proceedings brought by the Secretary of State.

18.5 Section 90(4) provides for the CSP to disclose the existence of a data retention notice with the permission of the Secretary of State. Such circumstances are likely to include disclosure:

- To a person (such as a system provider) who is working with the CSP to give effect to the notice;
- To relevant oversight bodies; and
- To other CSPs subject to a retention notice to facilitate consistent implementation of the obligations.

Part 4

General Matters

19 Costs

Making of contributions

19.1 Section 225 of the Act recognises that CSPs incur expenses in complying with requirements in the Act, including the disclosure of communications data in response to requests under Part 3 of the Act and notices to retain communications data under Part 4. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.

19.2 The following sections outline the circumstances where the Government will make contributions towards the costs of complying with the Act. CSPs who are required to retain communications data will inevitably be required to disclose communications data in response to lawful requests. In those circumstances the Government will make contributions towards the costs of both retaining and disclosing the data. However, not all CSPs that are required to disclose data will be required to retain it. In those circumstances they will can only be asked to disclose data that they retain for business purposes. For such CSPs, the Government will only make contributions towards the costs of disclosing the data in response to requests under Part 3 of the Act.

Contributions of costs for the acquisition and disclosure of communications data

19.3 Significant public funding is made available to CSPs to ensure that they can provide, outside of their normal business practices, an effective and efficient response to public authorities' necessary, proportionate and lawful requirements for the disclosure and acquisition of communications data in support of their investigations and operations to protect the public and to bring to justice those who commit crime.

19.4 An effective and efficient response requires the timely disclosure of communications data. In this code 'timely disclosure' means that ordinarily a CSP should disclose data within ten working days of being required to do so.

19.5 It is legitimate for a CSP to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to facilitate the timely disclosure of communications data.

19.6 This is especially relevant for CSPs which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems or where, in smaller CSPs, additional resources may be required to facilitate the response to such requests.

19.7 Contributions may also be appropriate towards costs incurred by a CSP which needs to update its systems to maintain, or make more efficient, its disclosure process. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the disclosure and acquisition of communications data relating to the use of such services.

19.8 Where a CSP identifies that a request for data may result in significant costs it may discuss this with the public authority before complying with the request. This may be a relevant consideration as to whether the request is reasonably practicable.

Costs in relation to a technical capability notice

19.9 CSPs that are subject to a technical capability notice under Part 9 of the Act are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a technical capability notice and the Act.

19.10 Any contribution towards these costs must be agreed by the Government before work is commenced by a CSP and will be subject to the Government considering, and agreeing, the technical capability proposed by the CSP.

19.11 Costs that may be recovered could include those related to the procurement or design of systems required to obtain communications data, their testing, implementation, continued operation and, where appropriate, sanitisation and decommissioning. Certain overheads may be covered if they relate directly to costs incurred by CSPs in complying with their obligations outlined above. This is particularly relevant for CSPs that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems.

Contributions of costs for the retention of communications data

19.12 The above considerations may be appropriate for all CSPs that are required to disclose data. The following considerations only apply to those CSPs that are subject to a retention notice under Part 4 of the Act. They are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a data retention notice and the Act.

19.13 Any contribution towards these costs must be agreed by the Home Office before work is commenced by a CSP and will be subject to the Home Office considering, and agreeing, the solution proposed by the CSP.

19.14 These costs may include the procurement or design of systems required to retain communications data, their testing, implementation, continued operation and where appropriate sanitisation and decommissioning. Some overheads may be covered if they directly relate to costs incurred by CSPs in complying with their obligations outlined above. Costs may also include costs related to feasibility studies conducted during the period in which a CSP is being consulted prior to a retention notice being served.

19.15 This is especially relevant for CSPs that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems or where, in smaller CSPs, additional resources may be required to comply with the requirements in a notice.

19.16 Contributions may also be appropriate towards the costs incurred by a CSP to update its systems to maintain, or make more efficient, its retention process. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the use of such services.

19.17 A data retention notice must specify the level or levels of contribution to be made in respect of the costs incurred in complying with the notice. Accordingly no changes can be made to the level of contribution without the data retention notice being varied.

General considerations on appropriate contributions

19.18 Any CSP seeking to recover appropriate contributions towards its costs should make available to the Government such information as the Government requires, in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the CSP.

19.19 As costs are reimbursed from public funds, CSPs should take into account value for money when procuring, operating and maintaining the infrastructure required to comply with a notice. As changes to business systems may necessitate changes to data retention and disclosure systems, CSPs should take this into account when altering business systems and should notify the Government of proposed changes which may affect the systems put in place to facilitate compliance under the Act. .

19.20 Any CSP that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

Power to develop compliance systems

19.21 In certain circumstances it may be more economical for products to be developed centrally rather than CSPs or public authorities creating multiple different systems to achieve the same end. Where multiple different systems exist it can lead to increased complexity, delays and higher costs in updating systems (such as for security updates).

19.22 Section 226 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop consistent systems to be used by CSPs or systems to be used by public authorities to acquire communications data. Such systems can operate in respect of multiple powers under the Act

19.23 Where such systems are developed for use in CSPs the Government will work closely with CSPs to develop systems which can be properly integrated into their networks. CSPs using such systems will have full sight of any processing of their data carried out by such systems. The Home Office should consult both the Investigatory Powers Commissioner and the Information Commissioner where relevant.

20 Referral of technical capability and data retention notices

20.1 The Act includes clear provisions for CSPs to request a review of the requirements placed on them in a technical capability notice or data retention notice should they consider these to be unreasonable. A person may refer the whole or any part of a notice back to the Secretary of State for review under the Act.

20.2 The circumstances and timeframe within which a CSP may request a review are set out in regulations made by the Secretary of State and approved by Parliament. These circumstances include opportunities for a CSP to refer a notice for review following the receipt of a new notice or the notification of a variation to a notice. Details of how to submit a notice to the Secretary of State for review will be provided either before or at the time the notice is served.

20.3 Before deciding the review, the Secretary of State must consult and take account of the views of the Technical Advisory Board (TAB) and a Judicial Commissioner. The Board must consider the technical requirements and the financial consequences of the notice for the person who has made the referral. The Commissioner will consider whether the notice is proportionate.

20.4 The Commissioner and the TAB must give the relevant CSP and the Secretary of State the opportunity to provide evidence and make representations to them before reaching their conclusions. Both bodies must report these conclusions to the person who made the referral and the Secretary of State.

20.5 After considering reports from the TAB and the Commissioner, the Secretary of State may decide to vary, revoke or confirm the effect of the notice.

20.6 In respect of technical capability notices, where the Secretary of State decides to confirm or vary the notice, the Investigatory Powers Commissioner must approve the decision.

20.7 Until this decision is made (in respect of data retention notices) or approved (in respect of technical capability notices), there is no requirement for the CSP to comply with the notice so far as referred. For example, if a notice covers a number of services and the referral relates to only one of those services then the CSP must continue to comply with the notice in relation to the other services covered by the notice.

20.8 Where a technical capability notice is subject to a review the duty to comply in section 63 remains in effect in relation to individual authorisations made under Part 3 of the Act.

20.9 Where a data retention notice applies to more than one CSP then only the provider(s) who refer the notice are not required to comply.

20.10 Where a referral is made in respect of a data retention notice the Information Commissioner should be notified.

21 Keeping of records

Records to be kept by a relevant public authority

21.1 Applications, authorisations, copies of notices, and records of the withdrawal of authorisations and the cancellation of notices, must be retained by the relevant public authority in written or electronic form, and physically attached or cross-referenced where they are associated with each other. The public authority should also keep a record of the date and, when appropriate to do so, the time when each notice or authorisation is given or granted, renewed or cancelled. Records kept by the public authority must be held centrally by the SPoC or in accordance with arrangements previously agreed with the Commissioner.

21.2 These records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, to carry out its functions[69]. Although records are only required to be retained for at least three years, it is desirable, if possible, to retain records for up to five years.

21.3 Where the records contain, or relate to, material obtained directly as a consequence of the execution of an interception warrant, those records must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 51 of the Act.

21.4 This code does not affect any other statutory obligations placed on public authorities to keep records under any other enactment. For example where applicable in England and Wales, the relevant test given in the Criminal Procedure and Investigations Act 1996 ('the CPIA') as amended and the code of practice under that Act. This requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor.

21.5 Each relevant public authority must also keep a record of the following information:

A. The number of applications submitted by an applicant to a SPoC seeking the acquisition of communications data (including orally);

B. The number of applications submitted by an applicant to a SPoC seeking the acquisition of communications data (including orally), which were referred back to the applicant for amendment or declined by the SPoC, including the reason for doing so;

C. The number of applications submitted to a designated senior officer for a decision to obtain communications data (including orally), which were approved after due consideration;

D. The number of applications submitted to a designated senior officer for a decision to obtain communications data (including orally), which were referred back to the applicant or rejected after due consideration, including the reason for doing so;

---

[69] The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is satisfied it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates. See section 67(5) of RIPA.

E. The number of notices requiring disclosure of communications data (not including urgent oral applications);

F. The number of authorisations of conduct to acquire communications data (not including urgent oral applications);

G. The number of authorisations to issue a notice to acquire communications data (not including urgent oral applications);

H. The number of times an urgent authorisation is granted orally;

I. The number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data;

J. The priority grading of the application for communications data;

K. Whether any part of the application relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion) (and if so, which profession)[70];

L. The number of times an authorisation is granted to obtain communications data in order to confirm or identify a journalist's source; and

M. The number of items of communications data sought, for authorisation granted (including orally)[71].

21.6 For each **item** of communications data included within a notice or authorisation, the relevant public authority must also keep a record of the following:

A. The unique reference number (URN) allocated to the application, notice and/or authorisation;

B. The statutory purpose for which the item of communications data is being sought, as set out at section 58(7) of the Act;

C. Where the item of communications data is being sought for the purpose of preventing or detecting crime or of preventing disorder, as set out at section 58(7) of the Act, the crime type being investigated;

D. Whether the item of communications data is events or entity, as described at section 237(5) of the Act, and chapter 2 of this code;

E. A description of the type of each item of communications data included in the notice or authorisation[72];

F. Whether the item of communications data relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;

G. The age of the item of communications data. Where the data includes more than one day, the recorded age of data should be the oldest date of the data sought;

---

70 See paragraphs 6.1 – 6.4 on communications data involving certain professions for more information.

71 One item of communications data is a single communications address or other descriptor included in a notice or authorisation. For example, one communications address that relates to 30 days of incoming and outgoing call data is one item of communications data.

72 The data type is to include whether the data is telephone data, whether fixed line or mobile, or internet data. It will also include a further breakdown of the data type, such as, in the case of fixed line telephone data, whether the item of communications data relates to incoming call data, outgoing call data, or both. Guidance on specific data types to be collected may be issued by, or sought from the Commissioner.

H. Where an item of data is entity data retained by the CSP, an indication of the total number of days of data being sought by means of notice or authorisation[73]; and

I. The CSP from whom the data is being acquired.

21.7 These records must be sent in written or electronic form to the Investigatory Powers Commissioner, as determined by him. Guidance on record keeping will be issued by the Commissioner. Guidance may also be sought by relevant public authorities, CSPs or persons contracted by them to develop or maintain their information technology systems.

21.8 The Investigatory Powers Commissioner will not seek to publish statistical information where it appears to him that doing so would be contrary to the public interest, or would be prejudicial to national security.

Records to be kept by a communications service provider (acquisition)

21.9 To assist the Investigatory Powers Commissioner to carry out his statutory function in relation to communications data, CSPs should maintain a record of the disclosures they have made or been required to make. This record should be available to the Commissioner and his inspectors to enable comparative scrutiny of the records kept by public authorities. Guidance on the maintenance of records by CSPs may be issued by or sought from the Commissioner's Office.

21.10 The records to be kept by a CSP, in respect of each authorisation should include:

- The identity of the public authority;
- The URN of the authorisation;
- The date the authorisation was disclosed to the CSP;
- A description of any communications data required where no disclosure took place or could have taken place; and
- The date when the communications data was disclosed to the public authority or, where secure systems are provided by the CSP, the date when the acquisition and disclosure of communications data was undertaken.

21.11 CSPs should also keep sufficient records to establish the origin and exact communications data that has been disclosed in the event of later challenge in court. CSPs should retain this data for a period of up to two years. This may comprise data that was disclosed, a copy of the response, or a digital record that could be used to validate the response but should contain no more data than is necessary to verify the authenticity of such disclosures in court[74].

---

[73] In the case of a forward facing authorisation, the number of days of data sought will often differ from the number of days of data disclosed or acquired. This is because a forward facing authorisation will often be withdrawn or cancelled at the point it has served its purpose. For example, if the purpose is to identify an anticipated communication between two suspects, the authorisation may be withdrawn subsequent to that communication being made.

[74] A digital signature is an electronic record of a disclosure and would assist the court in verification of the origin and integrity of the data throughout the acquisition, investigation and prosecution process. Where a digital signature is held there should be no need to retain the underlying data.

21.12 A requirement to delete data at the end of the period of its retention specified under a retention notice does not apply to records held for this purpose.

Records to be kept by a communications service provider (retention)

21.13 To assist the Information Commissioner carry out his statutory function in relation to the Act, CSPs must maintain a record of information that indicates whether and how they have complied with the provisions of this code. Such information must be provided to him on request.

21.14 Such records may include but are not limited to:

- Data retention & disclosure system access audit records;
- IT Health Check security reports;
- Security incident logs;
- Data retention volumes;
- Details of retained financial records (i.e. PCI-DSS implications and required exemptions);
- Data destruction records;
- Hardware (storage media) destruction records; and
- Documentary evidence to demonstrate how the CSP has fulfilled its responsibilities under chapter 16 regarding security, integrity and destruction of retained data.

21.15 Guidance on the maintenance of records by CSPs to assist with the Information Commissioner's statutory functions in relation to the Act may be issued by or sought from him.

Errors

21.16 This section provides information regarding errors, which are not considered to meet the threshold of the offence detailed at paragraph 12.7.

21.17 Proper application of the Act and thorough procedures for operating its provisions, including the careful preparation and checking of applications, notices and authorisations, should reduce the scope for making errors whether by public authorities or by CSPs.

21.18 An error can only occur after a designated senior officer has granted an authorisation and the acquisition of data has been initiated.

21.19 Any failure by a public authority to apply correctly the process of acquiring or obtaining communications data set out in this code will increase the likelihood of an error occurring.

21.20 Where any error occurs in the granting of an authorisation, the giving of a notice or as a consequence of any authorised conduct – including use of the request filter, or any conduct undertaken to comply with a notice, a record should be kept.

21.21 Where an error results in communications data being acquired or disclosed wrongly, a report must be made to the Commissioner ('a reportable error'). Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, result in the individual being wrongly detained or wrongly accused of a crime as a result of that error.

21.22 In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ('recordable error'). These records must be available for inspection by the Commissioner.

21.23 'A reportable error' as set out in this code constitutes a relevant error for the purposes of section 209 of the Act (see section on serious errors beginning at paragraph 21.33).

21.24 This section of the code cannot provide an exhaustive list of possible causes of reportable or recordable errors. Examples could include:

Reportable errors

- An authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under the Act;
- Human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is acquired or disclosed;
- Disclosure of the wrong data by a CSP when complying with a notice;
- Acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation;and
- The omission of, or incorrect matches in filtered results, or the release of results that exceed specified thresholds.

Recordable errors

- A notice has been given which is impossible for a CSP to comply with and the public authority attempts to impose the requirement;
- Failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation[75];
- The requirement to acquire or obtain the data is known to be no longer valid;
- Failure to serve written notice (or where appropriate an authorisation) upon a CSP within one working day of urgent oral notice being given or an urgent oral authorisation granted;
- Where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly; and

[75] In this context seeking the disclosure of communications data unnecessarily means any failure to collate or record information already obtained which results in repeatedly obtaining the same data within the same investigation or operation. This does not restrict a relevant public authority undertaking the acquisition of communications data where necessary and proportionate, for example to extend the time frame of communications data already obtained, which may include elements of data previously obtained, or as a consequence of new evidence.

- Human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is not acquired or disclosed.

21.25 Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of communications data that require further improvement to eliminate errors and the risk of undue interference with any individual's rights.

21.26 When a reportable error has been made and identified, the public authority which made the error, or established that the error had been made, must establish the facts and report the error to the authority's senior responsible officer and then to the Commissioner within no more than five working days. All errors should be reported as they arise. If the report relates to an error made by a CSP, the public authority should also inform the CSP and Commissioner of the report in written or electronic form. This will enable the CSP and Commissioner to investigate the cause or causes of the reported error.

21.27 The report sent to the Commissioner by a public authority in relation to a reportable error must include details of the error, identified by the public authority's unique reference number of the relevant authorisation, explain how the error occurred, indicate whether any unintended collateral intrusion has taken place and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. When a public authority reports an error made by a CSP, the report must include details of the error and indicate whether the CSP has been informed or not (in which case the public authority must explain why the CSP has not been informed of the report).

21.28 Where a CSP discloses communications data in error, it must report each error to the Commissioner within no more than five working days of the error being discovered. It is appropriate for a person holding a suitably senior position within a CSP to do so, identifying the error by reference to the public authority's unique reference number and providing an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. Errors by service providers could include responding to a notice by disclosing incorrect data or by disclosing the required data to the wrong public authority[76].

21.29 In circumstances where a reportable error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal (see chapter 23).

21.30 The records kept by a public authority accounting for recordable errors must include details of the error, explain how the error occurred and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not reoccur. The authority's senior responsible officer must undertake a regular review of the recording of such errors.

21.31 Where material which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it is disclosed in error by a CSP, that material and any copy of it (including copies contained in or as attachments in electronic mail) should be destroyed as soon as the report to the Commissioner has been made.

21.32 Communications identifiers can be readily transferred, or 'ported', between CSPs. When a correctly completed authorisation or notice results in a CSP indicating to a public authority that, for example, a telephone number has been 'ported' to another CSP, that authorisation or notice will not constitute an error – unless the fact of the porting was already known to the public authority.

Serious errors

21.33 Section 209 of the Act states that the Commissioner must inform a person of any relevant error relating to that person which the Commissioner considers to be a serious error and that it is in the public interest for the person concerned to be informed of the error.

21.34 In circumstances where an error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

21.35 If the Commissioner concludes that the error has casued significant prejudice or harm to the person concerned, the Commissioner must also decide whether he considers that it is in the public interest for the person concerned to be informed of the error. In making this decision, the Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned; and
- The extent to which disclosing the error would be contrary to the public interest or prejudicial to:
  - national security;
  - the prevention or detection of serious crime;
  - the economic well-being of the United Kingdom; or
  - the continued discharge of the functions of any of the intelligence services.

21.36 Before making his or her decision, the Commissioner may require the public authority which has made the error to make submissions on the matters above.

Excess Data

21.37 Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority.

21.38 Where a public authority is bound by the Criminal Procedure and Investigations Act 1996 (CPIA) and its code of practice, there will be a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid authorisation. If a criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

21.39 If, having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The designated senior officer will then consider the reason(s) and review all the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. As with all communications data acquired, the requirements of the DPA and its data protection principles must also be adhered to in relation to any excess data.

Reporting of errors to the Information Commissioner

21.40 CSP are only required to report errors made in response to requests for communications data under Part 3 to the Investigatory Powers Commissioner. The Investigatory Powers Commissioner must consider whether any errors either reported or uncovered during inspections have resulted in personal data breaches that should be reported to the Information Commissioner, or whether details of the errors should be forwarded on because they are relevant to Information Commissioner's role under Part 4.

21.41 The Investigatory Powers Commissioner and the Information Commissioner should agree the circumstances under which information on errors should be forwarded.

22 Oversight

The Investigatory Powers Commissioner

22.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ('the Commissioner'), whose remit is to provide comprehensive oversight of the use of the powers contained within Parts 3 and 4 of the Act. By statute the Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work.

22.2 The Investigatory Powers Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The Commissioner may undertake these inspections, as far as they relate to the Commissioner's statutory functions, entirely on his or her own initiative or the Commissioner may be asked to investigate a specific issue by the Prime Minister.

22.3 The Commissioner will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the Commissioner must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers must, by law, offer all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

22.4 The Commissioner must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the national interest. Only the Prime Minister will be able to authorise redactions to the Commissioner's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

22.5 The Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publically available subject to public interest considerations. Public authorities and telecommunications operators may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce guidance for public authorities on how to apply and use Investigatory Powers. Wherever possible this guidance will be published in the interests of public transparency.

22.6 Section 215 provides that disclosures can be made to the Investigatory Powers Commissioner. This includes disclosures made by communications service providers who can contact the IPC at any time to request advice and guidance.

22.7 Anyone working for a public authority or communications service provider who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner, who will consider them. In particular, any person who exercises the powers described in the Act or whose activities are covered by this code must report to the Commissioner any action undertaken, which they believe to be contrary to the spirit or provisions of this code. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority. The Commissioner may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the Investigatory Powers Tribunal (IPT).

22.8 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to an individual who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the individual affected. Further information on errors can be found in chapter 21 of this code. The public body who has committed the error will be able to make representations to the Commissioner before they make their decision on whether it is in the public interest for the individual to be informed.

22.9 The Commissioner must also inform the affected individual of their right to apply to the Investigatory Powers Tribunal (see chapter 23 for more information on how this can be done) who will be able to fully investigate the error and decide if a remedy is appropriate..

22.10 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: [website for IPC once created]

The Information Commissioner

22.11 The Act requires that the Information Commissioner provides independent oversight of the integrity, security or destruction of data retained by virtue of part 4 of the Act. The role extends to all such data, irrespective of the system the data is retained in.

22.12 This code does not cover the exercise of the Information Commissioner's functions. It is the duty of any CSP subject to a notice under the Act to comply with any requests made by the Commissioner, in order to provide any information he requires to discharge his functions. The Commissioner may, for example, make requests:

- to access any relevant premises;
- for copies of relevant documentation;
- to inspect any relevant equipment or other material; or
- to observe the processing of relevant communications data.

22.13 Without prejudice to the independence of the Information Commissioner, if a CSP considers a request to be unreasonable they should refer the matter to the Home Office.

22.14 Reports made by the Information Commissioner concerning the inspection of CSPs and the security, integrity and destruction of communications data retained under the Act must be made available by the Information Commissioner to the Home Office. This can help to promulgate good practice and identify security enhancements and training requirements within CSPs. The Home Office will work with CSPs to address any recommendations made by the Information Commissioner.

22.15 Subject to discussion between the Information Commissioner and the Home Office, either may publish the inspection reports, in full or in summary, or a single overarching report to demonstrate both the oversight of the security, integrity and destruction of data and CSPs compliance with the Act. Because of the sensitivity of identifying which companies have received retention notices, any such report must be sufficiently redacted to protect the identities of the companies.

22.16 Section 90(3) of the Act prohibits the Information Commissioner or a member of his staff disclosing the existence of a retention notice or the content of the retention notice to any person without the permission of the Secretary of State.

Enforcement of integrity, destruction and security standards

22.17 The Act imposes a duty on CSPs to comply with requirements or restrictions imposed by the Act or a retention notice issued under the Act. That duty is enforceable by civil proceedings brought by the Secretary of State.

22.18 In the event of a failure to comply with the integrity, destruction and security requirements contained in the Act or in a retention notice, the Secretary of State will consider whether enforcement action is appropriate or whether to work with CSPs to address any issues identified in the first instance.

22.19 Additionally, should the Information Commissioner establish instances of failure to comply with the Data Protection Act 1998 or other relevant data protection legislation, he may take enforcement action using powers under that legislation.

22.20 Should the Information Commissioner identify any errors or issues relating to the disclosure of communications data he may take such steps as he considers necessary to bring them to the attention of the CSP. Chapter 21 of this code sets out the requirements on CSPs in relation to any such errors.

23 Contacts / Complaints

General enquiries relating to communications data retention and acquisition

23.1 The Home Office is responsible for policy and legislation regarding communications data acquisition and disclosure. Any queries should be raised by contacting:

Communications Data Policy Team
Home Office
2 Marsham Street
London
SW1P 4DF

commsdata@homeoffice.x.gsi.gov.uk

23.2 The Knowledge Engagement Team within the College of Policing can provide advice and guidance to police and other public authorities in relation to their obligations under communications data legislation. The Knowledge Engagement Team can be contacted at:

ketadmin@college.pnn.police.uk

Complaints

Data security, integrity and destruction

23.3 The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with these regulations. Failure to comply with this code's provisions in these areas may also engage concerns about compliance with data protection and related legislation. Any concerns about compliance with data protection and related legislation should be passed to the Information Commissioner's Office (ICO) at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

0303 123 1113

www.ico.org.uk

Acquisition and retention of communications data

23.4 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against public authority use of investigatory powers and human rights claims against the security and intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

23.5 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination.

23.6 This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: http://www.ipt-uk.com. Alternatively information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

23.7 If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

This code of practice relates to the powers and duties conferred or imposed under Parts 3 and 4 of the Investigatory Powers Act relating to the acquisition of communications data by public authorities and its disclosure by communications service providers, and to the retention of communications data by communications service providers.

It provides guidance on:

- procedures to be followed for the acquisition of communications data;
- rules for the granting of authorisations to acquire data and the giving of notices to require disclosure of data;
- procedures to be followed for the retention of communications data;
- security principles which must be adhered to by those retaining data;
- keeping of records, including records of errors; and
- the oversight arrangements in place for acquisition and retention of communications data.

This code is aimed at:

- members of public authorities who are involved in the acquisition of communications data whether as an applicant, a single point of contact, a designated senior officer or a senior responsible officer; and
- communications service providers' staff involved in the lawful disclosure of communications data or who currently, or may in the future, retain data under the Act.

Home Office

Bulk Acquisition

DRAFT Code of Practice

Autumn 2016

Bulk Acquisition

DRAFT Code of Practice

Published for consultation alongside the Investigatory Powers Bill

Autumn 2016

Contents

1 Introduction

1.1 This code of practice relates to the powers and duties conferred or imposed under Chapter 2 of Part 6 of the Investigatory Powers [Act 2016] ('the Act').

1.2 A bulk acquisition warrant under that Part is a warrant which authorises or requires the person to whom it is addressed to obtain the communications data described in the warrant from a communications service provider (CSP), as well as to access the acquired communications data, as specified in the warrant.

1.3 Throughout this code the data acquired under a bulk acquisition warrant is referred to as bulk communications data ('BCD').

1.4 This code applies to the Security and Intelligence Agencies ('SIA') and communications service providers[1] who have been issued with a warrant under Part 6, Chapter 2.

1.5 This code should be readily available to members of the SIA involved in the acquisition of communications data in bulk and its examination, and to CSPs involved in the disclosure of this data to a member of the SIA under the Act. The Act provides that persons exercising any functions to which this code relates must have regard to the code. Although failure to comply with the code does not, of itself, make a person liable to criminal or civil proceedings.

1.6 The Act provides that the code is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to a question before any court or tribunal hearing any such proceedings, or to the Investigatory Powers Tribunal (the 'IPT') or to the Investigatory Powers Commissioner ('the Commissioner') or the Information Commissioner when overseeing the powers conferred by the Act, it may be taken into account.

1.7 The exercise of powers and duties under Chapter 2 of Part 6 of the Act and this code are kept under review by the Investigatory Powers Commissioner appointed under section 205 of the Act and by his Judicial Commissioners and inspectors who work from the Investigatory Powers Commission (the 'IPC').

1.8 The Home Office may issue further advice directly to the SIA and CSPs as necessary.

1.9 This code extends to the United Kingdom[2].

1.10 For the avoidance of doubt, the guidance in this code takes precedence over any contrary content of a public authority's internal advice or guidance.

---

[1] See paragraph 2.1

[2] This code and the provisions in Parts 3 and 4 of the Act do not extend to the Crown Dependencies and British Overseas Territories.

2 Scope and definitions

Communications service provider

2.1 The obligations under Parts 3 and 4 of the Act apply to telecommunications operators and postal operators. Throughout this code, communications service provider ('CSP') is used to refer to a telecommunications operator or postal operator. CSP is not a term used in the Act.

2.2 A telecommunications operator is a person who offers or provides a telecommunication service to persons in the UK or who controls or provides a telecommunication system which is, (in whole or in part) in or controlled from the UK. A postal operator is a person providing a postal service to a person in the UK. These definitions make clear that obligations in the Parts of this Act to which this code apply cannot be imposed on communications service providers whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK.

2.3 Section 237 of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the telecommunication service provider); and defines 'telecommunications system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. The definition of 'telecommunications service' in the Act is intentionally broad so that it remains relevant for new technologies.

2.4 The Act makes clear that any service which consists in, or includes, facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunications system is included within the meaning of 'telecommunications service'. Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.

2.5 The definition of a telecommunications operator also includes application and website providers but only insofar as they provide a telecommunication service. For example an online market place may be a telecommunications operator as it provides a connection to an application/website. It may also be a telecommunications operator if and in so far as it provides a messaging service.

2.6 Telecommunications operators may also include those persons who provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in commercial premises such as hotels or public premises such as airport lounges or public transport.

2.7 In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider, or where there are security implications in doing so, the data may be sought from the CSP which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of communications data for example where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room.

Composition of communications

2.8 For the purposes of the Act communications may comprise two broad categories of data: systems data and content. Some communications may consist entirely of systems data. Section 237(6)(b) makes clear that anything which is systems data is, by definition, not content. When permitted by the Act, certain data may also be separated from the remainder of a communication in circumstances where, if it were so separated, it would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication. This is identifying data. Systems data and identifying data may be obtained by interception or equipment interference warrants under Parts 2 and 5, and 6 of the Act. Further details on systems and identifying data can be found in the interception and equipment interference codes of practice.

2.9 Communications data is a subset of systems data. Section 237(5) is clear that, even though systems data cannot be content, communications data is limited to data which does not reveal anything of what might reasonably be considered to be the meaning of the communication, excepting any meaning arising from the fact of the communication or transmission of the communication. That is, any systems data which would, in the absence of section 237(6)(b), be content, cannot be communications data.

2.10 Any communications data obtained as part of systems data under an interception warrant is intercept material. Any such data must be treated in accordance with the restrictions on the use of intercept material in the Interception Code of Practice. Communications data obtained as part of systems data under an equipment interference warrant must be handled in accordance with the safeguards set out in the Equipment Interference Code of Practice.

Communications data

2.11 The term ‘communications data’ includes the ‘who’, ‘when’, ‘where’, and ‘how’ of a communication but not the content i.e. what was said or written[3].

2.12 It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning[4], of the communication.

---

[3] See paragraph 2.26 for the definition of content.

[4] As set out at section 237(6)(a).

2.13 It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

2.14 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services – i.e. postal services or telecommunications services.

2.15 Communications data about postal services cannot be acquired using a warrant issued under Chapter 2 of Part 6 of the Act.

2.16 Communications data in relation to telecommunications operators' services and systems includes data held or obtainable by a CSP or which is available directly from a telecommunications system and which:

- is about an entity to which a telecommunication service is provided **and** relates to the provision of the service;
- is comprised in, included as part of, attached to or logically associated with a communication for the purposes of a telecommunication system that facilitates the transmission of that communication; or
- relates to the use of a service or system; or
- is about the architecture of a telecommunication system.

2.17 The first limb of the definition includes information about any person to whom a service is provided, whether a subscriber or guest user and whether or not they have ever used that service. For example this may include information about the person associated with an email address even if that email address has not been used since its creation.

2.18 An entity can also include devices so this limb would cover information about the devices owned by a customer as well as the services to which the owner of the devices subscribes. This data may include names and addresses of subscribers.

2.19 Importantly this limb is limited to data held or obtained by the CSP in relation to the provision of a telecommunications service – it does not include data which may be held about a customer by a CSP more generally which are not related to the provision of a telecommunications service. For example, for a social media provider data such as the status of the account, contact details for the customer and the date a person registered with the service would all be communications data as they relate to the use of the service. However, other data held by the provider about a customer which does not relate to the provision of the telecommunication service, including personal information such as political or religious interests included in profile information, is not within scope of the definition of communications data.

2.20 The second limb includes any information that is necessary to get a communication from its source to its destination, such as dialled telephone number or internet protocol (IP) address. It includes data which:

- identifies the sender or recipient of a communication or their location;
- identifies or selects the apparatus used to transmit the communication;

- comprises signals which activate the apparatus used (or which is to be used to) to transmit the communication; and
- identifies data as being part of a communication.

2.21 Communications data under this limb also includes data held or capable of being obtained, by the CSP which is logically associated with a communication for the purposes of the telecommunications system by which the communication is being, or may be, transmitted. This might include, for example domain name service (DNS) requests which allow communications to be routed across the network. It also includes data that facilitates the transmission of future communications (regardless of whether those communications are, in fact, transmitted).

2.22 Only information falling within this second limb can be obtained directly from a telecommunications system by a public authority.

2.23 The third limb covers other information held by a CSP about the use of the service such as billing information.

2.24 The fourth limb additionally includes data held by a CSP about the architecture of the telecommunications system (sometimes referred to as 'reference data'). This may include the location of cell masts or Wi-Fi hotspots. This information itself does not contain any information relating to specific persons and its acquisition in its own right does not interfere with the privacy of any customers. However, this data is often necessary for the public authority to interpret the data received in relation to specific communications or users of a service.

2.25 Examples of communications data include, but are not limited to:

- 'subscriber checks' (also known as 'reverse look ups') such as "who is the subscriber of phone number 01632 960 224?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus/devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes[5];
- information about selection of preferential numbers or discount calls;
- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);

[5] This includes PUK (Personal Unlocking Key) codes for mobile phones. These are initially set by the handset manufacturer and are required to be disclosed in circumstances where a locked handset has been lawfully seized as evidence in criminal investigations or proceedings.

- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- itemised telephone call records (numbers called)[6];
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded; and
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

Content

2.26 The content of a communication is defined in 237(6) of the Act as the data which reveals anything of what might be reasonably be considered to be the meaning (if any) of that communication.

2.27 When one person sends a message to another, what they say or what they type in the subject line or body of an email is the content. However, there are many ways to communicate, and the definition covers the whole range of telecommunications. What is consistent is that the content will always be the part of the communication (whether it be the speech of a phone call or the text of an email) that conveys the substance or meaning of the sender is intending to convey to the recipient. It is that meaning that the Act defines as content.

2.28 When a communication is sent over the telecommunication systems it can be carried by multiple providers. Each provider may need a different set of data in order to route the communication to its eventual destination. Where data attached to a communication is identified as communications data it continues to be communications data, even if certain providers have no reason to look at this data. The definition of content ensures that the elements of a communication which are considered to be content do not change depending on which communication provider is carrying the communication.

2.29 There are two exceptions to the definition of content (set out in section 237(6)). The first addresses inferred meaning. When a communication is sent, the simple fact of the communication conveys some meaning, e.g. it can provide a link between persons or between a person and a service. This exception makes clear that any communications data associated with the communication remains communications data and the fact that some meaning can be inferred from it does not make it content.

---

[6] Itemised bills can include an indication of the cost for receiving communications, for example calls and messages received by a mobile telephone that has been ‘roaming’ on another network.

2.30 The second makes clear that systems data cannot be content[7].

Guidance on definitions

2.31 The Home Office may, from time to time, issue further guidance to CSPs or public authorities, on how the definitions in the Act apply.

[7] See interception and equipment interference codes of practice for more information.

3 General information on bulk acquisition

3.1 Bulk acquisition warrants authorise a two stage process. First, the obtaining of BCD from a CSP and second, the selection for examination of the BCD obtained under the warrant.

3.2 A bulk acquisition warrant will be served on a CSP to require that CSP to disclose the communications data specified in the warrant. This may also require a CSP to obtain and disclose specified communications data that is not in its possession but that it is capable of obtaining.

3.3 A warrant will normally provide for the provision of communications data as it is generated or processed by the CSP for business purposes, but may also relate to the provision in bulk of communications data retained by a CSP for business purposes or under the provisions in Part 4 of the Act. This may result in the collection of large volumes of communications data. This is essential to enable communications relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation.

3.4 In contrast to a targeted communications data authorisation, issued under Part 3 of the Act, a bulk acquisition warrant instrument need not be constrained to a specific operation.

3.5 Chapter 2 of Part 6 does not impose a limit on the volume of communications data which may be acquired. For example, if the requirements of this chapter are met then the acquisition of all communications data generated by a particular CSP could, in principle, be lawfully authorised but only where necessary and proportionate[8] to do so. This reflects the fact that bulk acquisition is an intelligence gathering capability, whereas targeted communications data acquisition is primarily an investigative tool that is used to acquire data in relation to specific investigations.

3.6 Accordingly, and in contrast to targeted communications data acquisition, a warrant may only be sought by a member of the SIA. In addition, the volume of data which may potentially be acquired is reflected in that fact that bulk acquisition warrants must be granted by the Secretary of State and are subject to approval by the Judicial Commissioner. Once acquired in bulk, selection of data for examination is only permitted for approved operational purposes.

3.7 In contrast to the bulk powers provided for in Chapters 1 and 3 of Part 6 of the Act, a bulk acquisition warrant may relate to communications data in relation to individuals in the UK.

[8] See paragraphs 3.8-3.11.

Necessity and proportionality

3.8 Obtaining of BCD will almost always involve an interference with an individuals' rights under Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR). This would only be justifiable if the conduct is necessary for a legitimate purpose and proportionate to that purpose. The Act recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the following statutory purposes set out in the Act:

- In the interests of national security, which must always be one of the purposes;
- For the purpose of preventing or detecting serious crime. Serious crime is defined in section 239(1) as crime that comprises an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; or
- In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security. The power to issue a bulk acquisition warrant for the purpose of safeguarding the economic well-being of the UK may only be exercised where it appears to the Secretary of State and Judicial Commissioner that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant for these purposes if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant for the purpose of safeguarding the economic well-being of the UK should therefore identify the circumstances that are relevant to the interests of national security. The power to issue a bulk acquisition warrant for the purpose of safeguarding the economic well-being of the UK may also only be exercised in circumstances where the information it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.

3.9 The Secretary of State must also believe that the acquisition of data 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 those whose data may be obtained 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 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.

Is the investigatory power under consideration appropriate in the specific circumstances?

3.10 No interference with privacy should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.11 The following elements of proportionality should therefore be considered:

- Balancing the extent of the proposed interference with privacy against what is sought to be achieved;

- Explaining how and why the methods to be adopted will cause the least possible interference on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
- Evidencing, as appropriate, what other methods have been considered and were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the use of the proposed investigatory power.

Trade Unions

3.12 As set out in clause 147, the fact that the information that would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State. The security and intelligence agencies are permitted to apply for a warrant against members or officials of a trade union considered to be a legitimate intelligence target where that is necessary for one of the statutory purposes and proportionate to what is sought to be achieved.

4 Giving of bulk acquisition warrants

Application for a bulk acquisition warrant

4.1 An application for a bulk acquisition warrant is made to the Secretary of State. As set out in section 147 of the Act, bulk acquisition warrants are only available to the intelligence agencies. An application for a bulk acquisition warrant therefore may only be made by or on behalf of the following persons:

- The Director General of the Security Service;
- The Chief of the Secret Intelligence Service; or
- The Director of the Government Communications Headquarters (GCHQ).

4.2 Bulk acquisition warrants, when issued, are addressed to the person who submitted the application. A copy of the warrant, or part of the warrant, may then be served on any person who may be able to provide assistance in giving effect to that warrant.

4.3 Prior to submission, each application is subject to a review within the agency making the application. This involves consideration of whether the application is necessary for one or more of the permitted statutory purposes (in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security). One of the statutory purposes for which a bulk acquisition warrant can be issued must always be national security.

4.4 The scrutiny of the application will also include whether the proposed acquisition of communications data in bulk is both necessary and proportionate and whether the examination of that material is, or may be, necessary for one or more of the operational purposes specified.

4.5 Each application, a copy of which must be retained by the applicant, should contain the following information:

- Description of the BCD to be acquired, details of any CSP(s) and an assessment of the feasibility of the operation where this is relevant and to the extent known at the time of the application[9];
- Description of the conduct to be authorised, which must be restricted to the obtaining of BCD, or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant;
- The operational purposes for which the BCD may be selected for examination;
- An explanation of why the acquisition of BCD is considered to be necessary for one or more of the statutory purposes, which must always include an explanation of why the acquisition of the data is necessary in the interests of national security;

[9] This assessment is normally based upon information provided by the relevant communications service provider.

- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, explaining why less intrusive alternatives have not been or would not be as effective;
- An assurance that the BCD will be selected for examination only so far as it is necessary for one or more of the operational purposes specified in the warrant and it meets the conditions of section 160 of the Act; and
- An assurance that all BCD will be kept for no longer than necessary and handled in accordance with the safeguards required by section 159 of the Act.

Format of a bulk acquisition warrant

4.6 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 warrant. CSPs will not receive a copy of the operational purposes specified in the warrant. The warrant should include the following:

- A description of the communications data to be acquired;
- The steps a CSP must take to give effect to the warrant;
- The operational purposes for which any BCD obtained under the warrant may be selected for examination;
- The warrant reference number; and
- Details of the persons who may subsequently modify the operational purposes specified on the warrant in an urgent case.

Authorisation of a bulk acquisition warrant

Necessity

4.7 Before issuing a warrant under Chapter 2 of Part 6 of the Act, the Secretary of State and Judicial Commissioner must consider that the warrant is necessary for one or more of the statutory purposes, as at sections 147(1)(a) and 147(2). If the Secretary of State or Judicial Commissioner is not satisfied that the warrant is necessary in the interests of national security, then it cannot be issued.

4.8 Before issuing a bulk acquisition warrant, the Secretary of State and Judicial Commissioner must also consider that the selection for examination of BCD obtained under the warrant is necessary for one or more of the specified operational purposes (section 147(1)(c)). Setting out the operational purposes on the warrant limits the purposes for which BCD collected under the warrant can be selected for examination. When considering the specified operational purposes, the Secretary of State and Judicial Commissioner must also be satisfied that selection for examination of BCD is necessary for one or more of the statutory purposes set out on the warrant (as at 147(1)(a) and 147(2)). For example, if a bulk acquisition warrant is issued in the interests of national security and for the purpose of preventing or detecting serious crime, every specified operational purpose on that warrant must be necessary for one or both of these two broader purposes.

4.9 The Secretary of State has a duty to ensure that arrangements are in force for securing that only that material which has been considered necessary for examination for a section 147(1)(a) or section 147(2) purpose, and which meets the conditions set out in section 160 is, in fact, selected for examination. The Investigatory Powers Commissioner is under a duty to review the adequacy of those arrangements.

Proportionality

4.10 In addition to the consideration of necessity, the Secretary of State and Judicial Commissioner must be satisfied that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

4.11 In considering whether a bulk acquisition warrant is necessary and proportionate, the Secretary of State and Judicial Commissioner must take into account whether the information it is considered necessary to obtain under the warrant could reasonably be obtained by other means (section 147(5) of the Act). This consideration should include whether the required information could reasonably be obtained through a less intrusive power such as the targeted acquisition of communications data or the targeted acquisition of communications data using the request filter.

Safeguards

4.12 Before issuing a warrant, the Secretary of State must consider that satisfactory arrangements are in force in relation to the warrant setting out the safeguards for the copying, dissemination, retention and access to BCD. These safeguards are explained at chapters 8 and 9 below.

Judicial Commissioner approval

4.13 Following the decision to issue a bulk acquisition warrant by the Secretary of State, it must be approved by a Judicial Commissioner.

4.14 Section 148 of the Act sets out the factors that a Judicial Commissioner must consider when deciding whether to approve the decision to issue a bulk acquisition warrant. The Commissioner must review the Secretary of State's conclusions as to:

- whether the warrant is necessary and the conduct it authorises is proportionate to what is sought to be achieved; and
- the necessity of examination for each of the specified operational purposes, including whether those operational purposes are necessary for the statutory purposes on the warrant.

4.15 In reviewing these factors, the Judicial Commissioner must apply judicial review principles to a sufficient degree to ensure compliance with the general duties in relation to privacy imposed by section 2 of the Act. The Judicial Commissioner may speak to the warrant granting department or warrant seeking agency as part of their considerations.

4.16 If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either:

- not issue the warrant; or

- refer the matter to the Investigatory Powers Commissioner for a decision (unless the Investigatory Powers Commissioner has made the original decision).

4.17 If the Investigatory Powers Commissioner refuses the decision to issue a warrant the Secretary of State must not issue the warrant.

5 Modifications, renewals, and cancellation

Modification of a bulk acquisition warrant

5.1 A bulk acquisition warrant may be modified by an instrument issued by the person permitted to do so under the provisions at section 153 of the Act. A bulk acquisition warrant may be modified to add, vary or remove an operational purpose for which BCD obtained under the warrant may be selected for examination.

5.2 If an agency requires a change in the scope of the data to be obtained under a warrant or a change to the statutory purpose for which the warrant is issued then an additional or replacement warrant must be sought. Nothing in section 153 of the Act permits, by modification, the addition of an operational purpose which is not relevant to the statutory purposes in relation to which the warrant has been issued.

5.3 In circumstances where a modification is being made to add or vary an operational purpose, the modification must be made by a Secretary of State and must be approved by a Judicial Commissioner before the modification comes into force. The considerations set out in chapter 4 apply to a modification as they do to the issuing of a new warrant.

5.4 In circumstances where a bulk acquisition warrant is being modified to remove an operational purpose, the modification may be made by the Secretary of State or by a senior official acting on their behalf. If a modification, removing an operational purpose is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it. If at any time the Secretary of State, or a senior official acting on their behalf, considers that a specified operational purpose is no longer necessary in the interests of the statutory purposes listed on the warrant, they shall modify the warrant to remove that operational purpose.

5.5 As set out above, a bulk acquisition warrant authorises a two stage process; the acquisition of BCD, followed by the selection for examination of the material collected under the warrant. There will be limited circumstances where it may no longer be necessary, or possible, to continue the first stage of this process, such as where the communications service provider providing assistance with giving effect to the warrant has ceased business. In such circumstances, it may continue to be necessary and proportionate to select for examination the material collected under that warrant. The Act therefore provides that a bulk acquisition warrant can be modified such that it no longer authorises the acquisition of BCD but continues to authorise selection for examination.

5.6 Such a modification may be made by the Secretary of State or by a senior official acting on their behalf. In circumstances where such a modification is being made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

Urgent modifications of a bulk acquisition warrant

5.7 In urgent cases a modification adding or varying an operational purpose can be made by a Secretary of State or a senior official with the express authorisation of the Secretary of State. An urgent case may be where a sudden terrorist incident requires the urgent selection for examination of the data already held for an operational purpose not listed on the warrant.

5.8 In these cases a statement of that fact must be endorsed on the modifying instrument, and the modification ceases to have effect after five working days following the date of issue unless it is approved by a Judicial Commissioner. If a Judicial Commissioner refuses to approve the modification, the modification will cease. Any collection of material between the modification being made and the Judicial Commissioner reviewing and refusing the modification will be lawful.

Renewal of a bulk acquisition warrant

5.9 The Secretary of State may renew a warrant within the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect (section 152 of the Act), with the approval of the Judicial Commissioner. Applications for renewalsare made to the Secretary of State and contain an update of the matters outlined in paragraph 4.5 above. In particular, the applicant must give an assessment of the value of the BCD obtained under the warrant to date and explain why it is considered that obtaining the data continues to be necessary in the interests of national security as well as, where applicable, either or both of the purposes in section 147(2), and why it is considered that obtaining of communications data in bulk continues to be proportionate.

5.10 In deciding to renew a bulk acquisition warrant, the Secretary of State must also consider that the selection for examination of BCD obtained under it continues to be necessary for one or more of the specified operational purposes, and that any examination of that material for these purposes is necessary for one or more of the statutory purposes (at 147(1)(a) and 147(2)) on the warrant.

5.11 In the case of a renewal of a bulk acquisition warrant that has been modified so that it no longer authorises or requires the acquisition of BCD, it is not necessary for the Secretary of State to consider that acquisition of BCD continues to be necessary before making a decision to renew the warrant.

5.12 Where the Secretary of State and Judicial Commissioner are satisfied that the warrant continues to meet the requirements of the Act, the Secretary of State may renew it. The renewed warrant is valid for six months from the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed

5.13 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 the instrument.

Warrant cancellation

5.14 The Secretary of State, or a senior official acting on their behalf, may cancel a bulk acquisition warrant at any time. Such persons must cancel a bulk acquisition warrant if, at any time before its expiry date, they are satisfied that the warrant is no longer necessary on the purposes of any one of the statutory purposes (at 147(1)(a) and 147(2)) for which it was issued. Such persons must also cancel a warrant if, at any time before its expiry date, he or she is satisfied that the examination of BCD is no longer necessary for any of the operational purposes specified on the warrant. Agencies will therefore need to keep their warrants under continuous review and must notify the Secretary of State if they assess that the warrant 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.

5.15 The cancellation instrument will be addressed to the person to whom the warrant was issued. A copy of the cancellation instrument should be sent to those CSPs who have given effect to the warrant during the preceding twelve months.

5.16 The cancellation of a warrant does not prevent the Secretary of State, with Judicial Commissioner approval, issuing a new warrant, covering the same, or different data and operational purposes, in relation to the same CSP in the future should it be considered necessary and proportionate to do so.

5.17 Where there is a requirement to modify the warrant, other than to vary the operational purposes for which the data can be selected for examination, then the warrant may be cancelled and a new warrant issued in its place.

6 Implementation of warrants and CSP compliance

6.1 After a warrant has been issued it will be forwarded to the person to whom it is addressed – i.e. the requesting agency which submitted the application.

6.2 Section 158 of the Act then allows the agency to carry out the acquisition of BCD, or to require the assistance of other persons in giving effect to the warrant. Section 158 makes clear that the warrant may be served on any person, inside or outside the UK, who is required to provide assistance in relation to that warrant.

6.3 Where a copy of the warrant has been served on a CSP, 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.

6.4 The implementing authority must take steps to bring the contents of the warrant to the attention of the relevant person. The Act provides that service of a copy of a warrant on a person outside the UK may (in addition to electronic or other means of service) be effected in any of the following ways:

- By serving it at the person's principal office within the UK or, if the person does not have an office in the UK, at any place in the UK where the person carries on business or conducts activities;
- At an address in the UK specified by the person;
- By making it available for inspection at a place in the UK (if neither of the above two methods are reasonably practicable). The implementing authority must take steps to bring the contents of the warrant to the attention of the relevant person.

6.5 The duty of compliance is enforceable against a person in the UK by civil proceedings by the Secretary of State for an injunction, or in Scotland for specific performance of a statutory duty under section 45 of the Court of Session Act 1988 or for any other statutory relief.

Provision of reasonable assistance to give effect to a warrant

6.6 Any CSP may be required to provide assistance in giving effect to a bulk acquisition warrant. A warrant can only be served on a person who is capable of providing the assistance required by the warrant. Section 158 places a requirement on CSPs to take all such steps for giving effect to the warrant as are notified to them. The duty to comply with the warrant can only be enforced against a person who is capable of complying with it. Where a technical capability notice is in place, a CSP will be considered to have put in place the capabilities specified in that notice when consideration is given to their compliance with the obligation.

6.7 The steps which may be required are limited to those which it is reasonably practicable to take (section 158(3)). What is reasonably practicable should be agreed after consultation between the CSP and the Government. Such consultation is likely to include consideration of a number of factors including, but not limited to, the technical feasibility and likely cost of complying with any steps notified to the CSP. As part of the consultation, the CSP may raise any other factor that they consider relevant to whether the taking of such steps is reasonably practicable. If no agreement can be reached it will be for the Secretary of State to decide whether to proceed with civil proceedings.

6.8 Where the relevant agency requires the assistance of a CSP in order to implement a warrant, it may provide the following to the CSP:

- A copy of the signed and dated warrant with the omission of the operational purposes and any or all of the other schedules; and/or
- A copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant. Warrants must specify the BCD to be obtained and the operational purposes for which any BCD obtained under the warrant may be selected for examination but CSPs will not receive a copy of the operational purposes specified in the warrant; and/or
- An optional covering document from the relevant agency (or the person acting on behalf of the agency) may also be provided requiring the assistance of the CSP and specifying any other details regarding the means of acquisition of the data and delivery as may be necessary. Contact details with respect to the relevant agency will be made available to the CSP.

Offence of unauthorised disclosure

6.9 A CSP served with a bulk acquisition warrant must keep the warrant secret. The offence of unauthorised disclosure occurs when any CSP, or employee of a CSP, reveals the content or existence of a warrant.

6.10 It is a reasonable excuse for a CSP to disclose the existence or content of a warrant with the permission of the Secretary of State. This is likely to include disclosure:

- To a person (such as a system provider) who is working with the CSP to give effect to the notice; and
- To relevant oversight bodies.

7 Maintenance of a technical capability

7.1 CSPs may be required under section 229 of the Act to provide a technical capability to give effect to interception, equipment interference, bulk acquisition warrants or communications data acquisition authorisations. The purpose of maintaining a technical capability is to ensure that, when a warrant or authorisation is served, companies can give effect to it securely and quickly. Small companies (under 10,000 users) will not be obligated to provide a permanent interception or equipment interference capability, although they may be obligated to give effect to a warrant.

7.2 The Secretary of State may give a relevant CSP a "technical capability notice" imposing on the relevant operator obligations specified in the notice, and requiring the person to take all steps specified in the notice, and requiring the person to take all steps specified in the notice. In practice, noticies will only be given to communications service providers that are likely to be required to give effect to warrants on a recurrent basis.

7.3 The obligations the Secretary of State considers reasonable to impose on such persons are set out in regulations made by the Secretary of State and approved by Parliament, and may include (amongst others) the obligations set out in section 229(4) of the Act:

- Obligations to provide facilities or services of a specified description;
- Obligations relating to apparatus owned or operated by a relevant operator;
- Obligations relating to the removal of electronic protection applied, by or on behalf of the relevant operator on whom the obligation has been placed, to any data;
- Obligations relating to the security of any postal or telecommunications services provided by the relevant operator; and
- Obligations relating to the handling or disclosure of any material or data.

7.4 An obligation placed on a CSP to remove encryption only relates to electronic protections that the company has itself applied to the data, or where those protections have been placed on behalf of that CSP. The purpose of this obligation is to ensure that the data can be provided in intelligible form. References to protections applied on behalf of the CSP include circumstances where the CSP has contracted a third party to apply electronic protections to a telecommunications service offered by that CSP to its customers.

7.5 In the event that a number of CSPs are involved in the provision of a service, the obligation to provide a capability, and to remove encryption, will be placed on the CSP which has the technical capability to give effect to the notice and on whom it is reasonably practicable to impose these requirements. It is possible that more than one communications service provider will be involved in the provision of the interception capability, particulalrly if more than one provider applies electronic protections to the relevant communications and secondary data.

7.6 While an obligation to remove encryption may only relate to protections applied by or on behalf of the company on whom the obligation is placed, there will also be circumstances where a CSP removes encryption from data for their own business reasons. Where this is the case a public authority will also require the CSP, where applicable and when served with a warrant, to provide that data in an intelligible form.

Consultation with service providers

7.7 Before giving a notice, the Secretary of State must consult the CSP. In practice, consultation is likely to take place long before a notice is given. The Government will engage with companies who are likely to be subject to a notice in order to provide advice and guidance, and prepare them for the possibility of receiving a notice.

7.8 In the event that the giving of a notice to a CSP is deemed appropriate, the Government will take steps to consult the company formally before the notice is given. Should the company have concerns about the reasonableness, cost or technical feasibility of requirements to be set out in the notice, these should be raised during the consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process.

Matters to be considered by the Secretary of State

7.9 Following the conclusion of consultation with a CSP, the Secretary of State will decide whether to give a notice. This consideration should include all the aspects of the proposed notice. It is an essential means of ensuring that the notice is necessary and proportionate to what is sought to be achieved and that proper processes have been followed.

7.10 As part of the decision the Secretary of State must take into account, amongst other factors, the matters specified in section 229(3):

- The likely benefits of the notice – this may take into account projected as well as existing benefits;
- The likely number of users (if known) of any telecommunications service to which the notice relates – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the technical capability notice;
- The technical feasibility of complying with the notice – taking into account any representations made by the communications service provider;
- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the company as part of the notice, such as those relating to security. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money; and
- Any other effect of the notice on the communications service provider – again taking into account any representations made by the company.

7.11 In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision. Clause 2 of the Act also requires the Secretary of State to have regard to the following when giving, varying or revoking a notice:

- Whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means
- The public interest in the integrity and security of telecommunications systems and postal services, and
- Any other aspects of the public interst in the protection of privacy.

7.12 The Secretary of State may give a notice after considering the points above if he or she considers that the notice is necessary, and that the conduct required is proportionate to what is sought to be achieved. The obligations set out in the notice must be reasonable, and the Secretary of State must ensure that communications service providers are capable of providing the necessary technical assistance.

7.13 Before the notice may be given, a Judicial Commissioner must approve the Secretary of State's decision to give a notice. In deciding whether to approve the Secretary of State's decision to give a relevant notice, a Judicial Commissioner must review the Secretary of State's conclusions regarding the necessity of the notice and the proportionality of the conduct required by the notice.

Giving a technical capability notice

7.14 Once a notice has been signed by the Secretary of State and the decision to give a notive has been approved by a Judicial Commissioner, arrangements will be made for this to be given to the communications service provider. During consultation, it will be agreed who within the company should receive the notice and how it should be issued (i.e. electronically or in hard copy). If no recipient is agreed, then the notice will be issued to a senior executive within the company.

7.15 Section 229(8) provides that obligations may be imposed on, and technical capability notices given to, a CSP located outside the UK and may require things to be done outside the UK. Where a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given to the CSP:

- 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; or
- At an address in the UK specified by the person.

7.16 As set out in section 229(7), the notice will specify the period within which the CSP must undertake the steps specified in the notice. It will often be the case that a notice will require the creation of dedicated systems. The time taken to design and construct such a system will be taken into account and, accordingly, different elements of the notice may take effect at different times.

7.17 A person to whom a technical capability notice is given is under a duty to comply with the notice. In respect of a technical capability notice to give effect to equipment interference or bulk acquisition warrants, the duty to comply with a technical capability notice is enforceable against a person in the UK by civil proceedings by the Secretary of State. The duty to comply with a technical capability notice to give effect to interception warrants and communications data authorisations is enforceable against a person in the UK and a person outside the UK by civil proceedings by the Secretary of State.

Disclosure of technical capability notices

7.18 The Government does not publish or release identities of those subject to a technical capability notice, as to do so may identify operational capabilities or harm the commercial interests of companies acting under a notice. Should criminals become aware of the capabilities of law enforcement, they may alter their behaviours and change CSP, making it more difficult to detect their activities of concern.

7.19 Any person to whom a technical capability notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence or contents of that notice to any person[10].

7.20 Section 231(8) of the Act provides for the person to disclose the existence and contents of a technical capability notice with the permission of the Secretary of State. Such circumstances are likely to include disclosure:

- To a person (such as a system provider) who is working with the CSP to give effect to the notice;
- To relevant oversight bodies;
- To regulators in exceptional circumstances where information relating to a capability may be relevant to their enquiries;
- To other CSPs subject to a technical capability notice to facilitate consistent implementation of the obligations; and
- In other circumstances notified to and approved in advance by the Secretary of State.

Regular review

7.21 The Secretary of State must keep technical capability notices under review. This helps to ensure that the notice itself, or any of the requirements or restrictions imposed by it, remains necessary and proportionate.

[10] See section 231(8)

7.22 It is recognised that, after a notice is given, a CSP is likely to require time to take the steps outlined in the notice and develop the necessary capabilities. Until these capabilities are fully operational, it will be difficult to assess the benefits of a notice. As such, the first review should not take place until after these are in place.

7.23 A review of a technical capability notice will take place at least once every two years once capabilities are in place. However, the exact timing of the review is at the Secretary of State's discretion.

7.24 A review may be initiated earlier than scheduled for a number of reasons. These include:

- a significant change in demands by agencies that calls into question the necessity and proportionality of the notice as a whole, or any element of the notice;
- a significant change in CSP activities or services; or
- a significant refresh or update of CSP systems.

7.25 The process for reviewing a notice is similar to the process for giving a notice. The Government will consult the communications service provider as part of the review. Once this process is complete, the Secretary of State will consider whether the notice remains necessary and proportionate.

7.26 A review may recommend the continuation, variation or revocation of a notice. The relevant communications service provider and the operational agencies will be notified of the outcome of the review.

Variation of technical capability notices

7.27 The communications market is constantly evolving and CSPs subject to technical capability notices will often launch new services.

7.28 CSPs subject to a technical capability notice must notify the Government of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require the CSP to provide a technical capability on the new service.

7.29 Small changes, such as upgrades of systems which are already covered by the existing notice, can be agreed between the Government and CSP in question. However, significant changes will require a variation of the technical capability notice.

7.30 Section 232 of the Act provides that technical capability notices can be varied by the Secretary of State. There are a number of reasons why a notice might be varied. These include:

- a CSP launching new services;
- changing demands and priorities of the security and intelligence agencies
- a recommendation following a review (see section beginning at 7.21); or
- to amend or enhance the security requirements.

7.31 Where a CSP has changed name, for example as part of a rebranding exercise or due to a change of ownership, the Government, in consultation with the CSP, will need to consider whether the existing notice should be varied.

7.32 Before varying a notice, the Government will consult the agencies to understand the operational impact of any change to the notice, and the CSPs to understand the impact on them, including any technical implications. Once this consultation process is complete, the Secretary of State will consider whether it is necessary to vary the notice and whether the new requirements imposed by the notice as varied are proportionate to what is sought to be achieved by that conduct.

7.33 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraphs 7.9 – 7.13.

7.34 Once a variation has been agreed by the Secretary of State, arrangements will be made for the CSP to receive notification of this variation and details of the timeframe in which the variation needs to be enacted by the CSP. The time taken to implement these changes will be taken into account and, accordingly, different elements of the variation may take effect at different times.

Revocation of technical capability notices

7.35 A technical capability notice must be revoked (in whole or in part) if it is no longer necessary to require a CSP to provide a technical capability.

7.36 Circumstances where it may be appropriate to revoke a notice include where a CSP no longer operates or provides the services to which the notice relates, where operational requirements have changed, or where such requirements would no longer be necessary or proportionate.

7.37 The revocation of a technical capability notice does not prevent the Secretary of State issuing a new technical capability notice, covering the same, or different, services to the same CSP in the future should it be considered necessary and proportionate to do so.

Referral of technical capability notices

7.38 The Act includes clear provisions for CSPs to request a review of the requirements placed on them in a technical capability notice should they consider these to be unreasonable. A person may refer the whole or any part of a technical capability notice back to the Secretary of State for review under section 233 of the Act.

7.39 The circumstances and timeframe within which a communications service provider may request a review are set out in regulations made by the Secretary of State and approved by Parliament. These circumstances include opportunities for a CSP to refer a notice for review following the receipt of a new notice or the notification of a variation to a notice. Details of how to submit a notice to the Secretary of State for review will be provided either before or at the time the notice is served.

7.40 Before deciding the review, the Secretary of State must consult and take account of the views of the Technical Advisory Board (TAB) and the Judicial Commissioner. The Board must consider the technical requirements and the financial consequences of the notice for the person who has made the referral. The Commissioner will consider whether the notice is proportionate.

7.41 Both bodies must give the relevant CSP and the Secretary of State the opportunity to provide evidence and make representations to them before reaching their conclusions. Both bodies must report these conclusions to the person who made the referral and the Secretaty of State.

7.42 After considering reports from the TAB and the Commissioner, the Secretary of State may decide to vary, withdraw or confirm the effect of the notice. Where the Secretary of State decides to confirm or vary the notice, the Investigatory Powers Commissioner must approve the decision.Until the Secretary of State's decision is approved, there is no requirement for the communciations service provider to comply with the notice so far as referred. The CSP will remain under obligation to provide assistance in giving effect to a bulk acquisition warrant, as set out in section 157 of the Act.

Contribution of costs for the maintenance of a technical capability

8.38 Section 225 of the Act recognises that communications service providers incur expenses in complying with requirements in the Act, including notices to maintain permanent interception capabilities under Part 9. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.

8.39 Communications service providers that are subject to a technical capability notice under Part 9 of the Act are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a technical capability notice and the Act.

8.40 Any contribution towards these costs must be agreed by the Government before work is commenced by a communications service provider and will be subject to the Government considering, and agreeing, the technical capability proposed by the communications service provider.

8 General safeguards

8.1 All BCD must be handled in accordance with safeguards which the Secretary of State has approved in line with the duty imposed on him or her by the Act. These safeguards are made available to the Investigatory Powers Commissioner, and they must meet the requirements of section 159 of the Act. Breaches of these safeguards must be reported to the Investigatory Powers Commissioner as agreed with him or her. The 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.

8.2 Section 159 of the Act requires that disclosure, copying and retention of BCD obtained under the warrant is limited to the minimum necessary for the authorised purposes. Section 159(3) of the Act provides that something is necessary for the authorised purposes if the BCD:

- Is, or is likely to become, necessary in the interests of national security or on any other purposes falling within section 147(2) – namely, 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[11];
- Is necessary for facilitating the carrying out of the functions under the Act of the Secretary of State or the person to whom the warrant is addressed;
- Is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal;
- Is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of him or her by his or her duty to secure the fairness of the prosecution; or
- Is necessary for the performance of any duty imposed by the Public Records Act.

Personnel security

8.3 All persons who may have access to BCD 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 BCD to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

[11] BCD obtained for one purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained for another.

Dissemination of BCD

8.4 BCD, and more typically the intelligence derived from it, will need to be disseminated both within and between agencies, as well as to consumers of intelligence, where necessary in order for action to be taken on it. The number of persons to whom a BCD set is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out in section 159(3) of the Act. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency.

8.5 It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: a BCD set 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 a BCD set to carry out those duties. In the same way, only so much of the BCD set may be disclosed as the recipient needs.

8.6 The obligations apply not just to the original recipient of the data, but also to anyone to whom the data is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

8.7 Section 159(9) of the Act stipulates that where BCD is disclosed to the authorities of a country or territory outside the UK, the appropriate agency must ensure BCD is only handed over to overseas authorities if the following requirements are met:

- It appears to the UK agency that the requirements corresponding to the requirements in 159(2) and 159(5) (relating to minimising the extent to which BCD is disclosed, copied, distributed and retained) will apply to the extent that the UK agency considers appropriate; and

- Restrictions are in force which would prevent, to such extent as the appropriate UK agency considers appropriate, the doing of anything in, for the purpose of or in connection with any proceedings outside the UK which would result in an unauthorised disclosure.

8.8 The material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the Secretary of State, and must be returned to the issuing agency or securely destroyed when no longer needed.

Copying

8.9 BCD may only be copied to the extent necessary for the authorised purposes set out in section 159(3) of the Act. This includes any record referring to a bulk acquisition warrant which includes the identities of the persons to or by whom the material was sent. The restrictions are implemented by requiring special treatment of such copies that are made by recording their making, distribution and destruction.

Storage and transfer of data

8.10 BCD, and all copies of it, must be handled and stored securely, so as to minimise the risk of loss or theft. In particular it must be held so as to be inaccessible to persons without the required level of vetting These requirements to store bulk communications data securely apply 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 officials before being asked to give effect to a warrant.

8.11 Individuals should be granted access only where it is required to carry out their function in relation to one of the authorised purposes set out in section 159(3) of the Act.

8.12 In particular, each agency must apply the following protective security measures:

- Physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems; and
- A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

8.13 BCD, and all copies, must be marked for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes. In this context, this means taking such steps as might be necessary to make access to the data impossible. If BCD is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 159(3) of the Act.

8.14 Where an agency obtains a BCD data set under a 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 Investigatory Powers 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 agency on the basis that continued retention of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue.

9 Safeguards when selecting BCD for examination

9.1 Section 160 of the Act provides specific safeguards relating to the selection for examination of BCD acquired through a bulk acquisition warrant.

9.2 Sections 160(1) and 160(2) make clear that selection for examination may only take place for one or more of the operational purposes that are specified on the warrant, in line with section 150 of the Act. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination, rather than limiting the information which can be examined per se, and no official is permitted to gain access to the data other than as permitted by these purposes. BCD selected for examination for an operational purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained on any relevant ground. Section 150 makes clear that operational purposes must relate to one or more of the statutory purposes specified on the warrant. However, it is not sufficient under the Act for operational purposes simply to use the wording of one of the statutory purposes. The Secretary of State may not approve the addition of an operational purpose to the central list – and therefore to any bulk warrants – unless he or she is satisfied that the operational purpose is specified in a greater level of detail than the relevant statutory purposes. Operational purposes must therefore describe a clear requirement and contain sufficient detail to satisfy the Secretary of State that intercepted content or secondary data may only be selected for examination for specific reasons.

9.3 Section 153 of the Act provides for a bulk acquisition warrant to be modified such that the operational purposes specified on it can be added to or varied. Such a modificiation is categorised as a major modification, and therefore must be made by the Secretary of State and approved by a Judicial Commissioner before the modification may take effect. In such circumstances, the provisions at section 153 also require that the operational purpose must be approved by the Secretary of State for addition to the central list. If the Secretary of State does not approve the addition of the purpose to the list, the modification to the warrant (to add a new operational purpose) may not be made. The Bill therefore creates a strict approval process in circumstances where an intelligence agency identifies a new operational purpose, which they consider needs to be added to a bulk warrant. The Secretary of State must agree that the operational purpose is a purpose for which selection for examination may take place, and that it is described in sufficient detail such that it should be added to the central list. In addition, the Secretary of State must also consider that the addition of that purpose to the relevant bulk warrant is necessary, taking into account the particular circumstances of the case, before making the modification, and the decision to add the operational purpose must also be approved by a Judicial Commissioner.

9.4 In addition to the central list of operational purposes having to be approved by the Secretary of State, section 153 makes clear that it must also be reviewed on an annual basis by the Prime Minister and it must be shared every three months with the Intelligence and Security Committee.

9.5 More than one operational purpose may be specified on a single bulk warrant; this may, where the necessity and proportionality test is satisfied, include all operational purposes currently specified on the central list maintained by the heads of the security and intelligence agencies. In the case of bulk acquisition, BCD relevant to a number of operational purposes may be acquired on a single warrant. In the majority of cases, it will therefore be necessary for bulk acquisition warrants to specify the full list of operational purposes.

9.6 As well as being necessary for one of the operational purposes, any selection for examination of BCD must be necessary and proportionate.

9.7 In general, automated systems must, where technically possible, be used to effect the selection of BCD in accordance with section 160 of the Act. As an exception, BCD may be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the material falls within the main categories to be selected under the specified operational purposes, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary for the purposes specified in sections 147(1)(a) and 147(2) of the Act.

9.8 Once those functions have been fulfilled, any copies made of the BCD for those purposes must be destroyed in accordance with section 159(5) of the Act. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the Investigatory Powers Commissioner during his or her inspections.

9.9 BCD should be selected for examination only by authorised persons who receive appropriate training regarding the provisions of the Act and specifically the operation of section 160 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.

9.10 Prior to an authorised person accessing the data a record[12] should be created setting out why access to BCD is required consistent with, and pursuant to, section 160 and the applicable operational purpose(s), and why such access is proportionate. Save where the material or automated systems are being checked as described in paragraph 9.9, 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. Where it is anticipated that the access to the BCD is likely to give rise to collateral intrusion to privacy, the reasons this is considered proportionate, and any steps to minimise it, must also be recorded. All records must be retained for the purposes of subsequent examination or audit.

[12] Any such record should be made available to the Commissioner on request for purposes of oversight.

9.11 Periodic audits should be carried out to ensure that the requirements set out in section 159 of the Act are being met. These audits must include checks to ensure that the records requesting access have been correctly compiled, and specifically, that the material requested falls within operational purposes the Secretary of State has considered necessary for examination. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards must be reported to the Investigatory Powers Commissioner. Where appropriate all intelligence reports generated by the authorised persons must be subject to a quality control audit.

9.12 The Secretary of State must ensure that the safeguards are in force before any acquisition under a bulk acquisition warrant can begin. The Investigatory Powers Commissioner is under a duty to review the adequacy of the safeguards. In particular, in reviewing the adequacy of bulk acquisition safeguards, the Commissioner should give specific consideration to the central list of operational purposes maintained by the heads of the security and intelligence agencies and the use of these purposes on bulk acquisition warrants.

Selection for examination of data relating to those in certain professions

9.13 The fact a communication took place does not disclose what was discussed, considered or advised.

9.14 However the degree of interference with an individual's rights and freedoms may be higher where BCD is being selected for examination with the intention of identifying data which relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament[13], or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.

9.15 Such situations do not preclude selecting the data for examination. However investigators, giving special consideration to necessity and proportionality, must take into account any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken when considering whether data should be selected for examination in such circumstances, including additional consideration of whether there might be unintended consequences of such examination and whether the public interest is best served by the data being selected for examination.

[13] References to a Member of Parliament include references to a Member of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

9.16 The nature of bulk data means that in many cases, the officer will not know who the communications data relates to at the point of its selection. However, officers must clearly note in all cases where it is intended or known that the data being selected for examination includes, or is likely to include, communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That fact that such data has been selected for examination must be recorded (see section 10 on keeping of records for more details), including recording the profession, and, at the next inspection, such records should be flagged to the Commissioner.

Selection for examination to determine the source of journalistic information

9.17 Issues surrounding the infringement of the right to freedom of expression may arise if BCD is selected for examination for the purpose of identifying the communications data of an identified or suspected journalist takes place. There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously. Where BCD is selected for examination in order to determine the source of journalistic information, there must therefore be an overriding requirement in the public interest.

9.18 A source of journalistic information is an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used. Throughout this code, references to sources should be understood to include any person acting as an intermediary between a journalist and a source.

9.19 An assessment of whether someone is a journalist (for the purposes of the Act) should be made on all the facts and circumstances available at that time. Consideration should be given, in particular, to the frequency of an individual's relevant activities, the level of professional rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest.In the exceptional event that an officer were to select for examination BCD specifically in order to determine a journalist's source, they should only do this if the proposal had been approved beforehand by a person holding the rank of Director or above within their organisation level. Any communications data obtained and retained as a result of such access must be reported to the Investigatory Powers Commissioner at the next inspection.

9.20 Communications data that may be considered to determine journalistic sources includes data relating to:

- journalists' communications addresses;
- the communications addresses of those persons suspected to be a source; and
- communications addresses of persons suspected to be acting as intermediaries between the journalist and the suspected source.

9.21 Where the officer suspects wrong-doing that includes communications with a journalist, the application must consider properly whether that conduct is of a sufficiently serious nature for rights to freedom of expression to be interfered with where communications data is to be selected for examination for the purpose of identifying a journalist's source.

9.22 The requirement for senior approval does not apply where the intent is to examine BCD to identify the communications data of a journalist, but it is not intended to determine the source of journalistic information (for example, where the journalist is suspected of involvement in terrorist activity).

9.23 In such cases there is nevertheless a risk of collateral intrusion into legitimate journalistic sources. In such a case, particular care must therefore be taken to ensure that the officer considers whether the intrusion is justified, giving proper consideration to the public interest. The officer needs to consider whether alternative evidence exists, or whether there are alternative means for obtaining the information being sought.

10 Record keeping and error reporting

Records

10.1 Records must be available for inspection by the Investigatory Powers Commissioner. The oversight regime allows the Investigatory Powers Commissioner to inspect the warrant application upon which the Secretary of State's decision is based, and the agency may be required to justify the content of the warrant.

10.2 Records must also be retained to allow the Investigatory Powers Tribunal, established under the Regulation of Investigatory Powers Act (RIPA), to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of RIPA), particularly where continuing conduct is alleged. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to five years.

10.3 Each agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:

- All applications made for bulk acquisition warrants, and applications made for the renewal of such warrants;
- All warrants, associated schedules 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 or Judicial Commissioner; and
- In relation to each warrant, the dates on which collection of BCD started and stopped.

10.4 Records should also be kept of the arrangements for securing that BCD has only been accessed for the specified operational purposes. Records should be kept of the arrangements by which the requirements of section 159(2) (minimisation of copying and distribution of bulk communications data), section 159(5) (destruction of bulk communications data) and section 160 (examination of bulk communications data) are to be met.

10.5 Records should also be kept by the relevant Department of State of the warrant authorisation process. This will include:

- All advice provided to the Secretary of State to support his/her consideration as to whether to issue or renew the bulk acquisition warrant; and
- Where the issuing of any application is not approved by the Judicial Commissioner, the grounds for refusal as given by the Judicial Commissioner and any associated advice/applications to the Investigatory powers Commissioner if there is an appeal.

10.6 Each agency must also keep a record of the information below for every calendar year to assist the Investigatory Powers Commissioner in carrying out his statutory functions:

- The number of applications made by or on behalf of the agency for a bulk acquisition warrant;
- The number of applications for a bulk acquisition warrant that were refused by a Secretary of State;
- The number of applications for a bulk acquisition warrant that were refused by a Judicial Commissioner;
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse a bulk acquisition warrant;
- The number of bulk acquisition warrants issued by the Secretary of State and approved by a Judicial Commissioner;
- The number of renewals to bulk acquisition warrants that were made;
- The number of bulk acquisition warrants that were cancelled; and
- The number of bulk acquisition warrants extant at the end of the year.

10.7 For each bulk acquisition warrant issued by the Secretary of State and approved by a Judicial Commissioner, the relevant agency must also keep a record of the following:

- The section 147(1)(a) and section 147(2) purpose(s) specified on the warrant;
- The details of modifications made to add, vary or remove an operational purpose from the warrant;
- The number of modifications made to add or vary an operational purpose that were made on an urgent basis;
- The number of modifications made to add or vary an operational purpose (including on an urgent basis) that were refused by a Judicial Commissioner; and
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse to modify a bulk acquisition warrant.

10.8 These records must be sent in written or electronic form to the Investigatory Powers Commissioner, as determined by him. Guidance on record keeping will be issued by the Investigatory Powers Commissioner. Guidance may also be sought from the Commissioner by agencies.

Errors

10.9 Proper application of the Act and thorough procedures for operating its provisions, including the careful preparation and checking of warrants and authorisations, should reduce the scope for making errors whether by public authorities or by CSPs.

10.10 An error can only occur after a warrant has been issued and the acquisition of data has been initiated.

10.11 Any failure by an agency to apply correctly the process of acquiring, or selecting for examination, BCD set out in this code will increase the likelihood of an error occurring.

10.12 Where any error occurs in the granting of a warrant, or any conduct undertaken to comply with a warrant, a record should be kept.

10.13 Where an error results in BCD being acquired or selected for examination wrongly, a report must be made to the Commissioner. Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, result in the individual being wrongly detained or wrongly accused of a crime as a result of that error. An error as set out in this code constitutes a relevant error for the purposes of section 209 of the Act (see section on serious errors beginning at paragraph 10.22).

10.14 This section of the code cannot provide an exhaustive list of possible causes of errors, however, examples could include:

BCD acquisition

- a warrant is not cancelled when the requirement to acquire the data is known to be no longer valid;
- human error, such as incorrect transposition of information from an application to a warrant where BCD is acquired; or
- over-collection caused by software or hardware issues.

BCD disclosure

- disclosure of the wrong data by a CSP when complying with the warrant; or
- disclosure of communications data by a CSP to the wrong public authority.

BCD access

- there has been material failure to adhere to the safeguards in sections 159 and 160 of the Act;
- communications data obtained under the warrant is selected on a basis that is not necessary and proportionate in all the circumstances; or
- selected communications data is examined on a basis that is not necessary for the fulfilment of one or more of the operational purposes specified in the warrant.

10.15 Reporting of errors will draw attention to those aspects of the process of acquisition of BCD that require further improvement to eliminate errors and the risk of undue interference with any individual's rights.

10.16 When an error has been made, the agency or other person which made the error (i.e. the CSP) must report the error to the Investigatory Powers Commissioner as soon as reasonably practicable after it has been established an error has occurred. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full.

10.17 All errors should be reported as they arise. If the report relates to an error made by a CSP, the public authority should also inform the CSP and Commissioner of the report in written or electronic form. This will enable the CSP and Commissioner to investigate the cause or causes of the reported error.

10.18 The report sent to the Commissioner by an agency in relation to an error must include details of the error, identified by the agency's unique reference number of the relevant authorisation, explain how the error occurred, indicate whether any unintended collateral intrusion has taken place and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. When an agency reports an error made by a CSP, the report must include details of the error and indicate whether the CSP has been informed or not (in which case the agency must explain why the CSP has not been informed of the report).

10.19 Where a CSP discloses BCD in error, it must report each error to the Commissioner within no more than five working days of the error being discovered. It is appropriate for a person holding a suitably senior position within a CSP to do so, identifying the error by reference to the relevant warrant and providing an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. Errors by service providers could include responding to a warrant by disclosing incorrect data or by disclosing the required data to the wrong agency[14].

10.20 In circumstances where a reportable error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal (see section 12).

10.21 Where material which has no connection to the data authorised for acquisition under the warrant obtained by an agency is disclosed in error by a CSP, that material and any copy of it (including copies contained in or as attachments in electronic mail) should be destroyed as soon as the report to the Commissioner has been made.

[14] This does not affect a CSPs statutory duty under regulation 5A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 to notify the Information Commissioner of a personal data breach. Further guidance is available from the Information Commissioner's website, ico.org.uk

Serious errors

10.22 Section 209 of the Act states that the Commissioner must inform a person of any relevant error relating to that person which the Commissioner consider to be a serious error and that it is in the public interest for the person concerned to be informed of the error.

10.23 In circumstances where an error is deemed to be of a serious nature, the Commissioner may therefore investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

10.24 If the Commissioner concludes that the error is a serious error, the Commissioner must also decide whether it considers that it is in the public interest for the person concerned to be informed of the error. The Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned; and
- the extent to which disclosing the error would be contrary to the public interest or prejudicial to:
  - national security
  - the prevention or detection of serious crime
  - the economic well-being of the United Kingdom; or
  - the continued discharge of the functions of any of the intelligence services.

10.25 Before making its decision, the Commissioner may require the agency which has made the error to make submissions on the matters above.

11 Costs

Making of contributions

11.1 Section 225 of the Act recognises that CSPs incur expenses in complying with warrants under Chapter 2 of Part 6 of the Act. The Act, therefore, allows for appropriate payments to be made to them to cover these costs. The following sections outline the circumstances where the Government will make contributions towards the costs of complying with the Act.

11.2 Significant public funding is made available to CSPs to ensure that they can provide, outside of their normal business practices, an effective and efficient response to warrants. It is legitimate for a CSP to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to facilitate the timely disclosure of the BCD specified in the warrant.

11.3 This is especially relevant for CSPs which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems. Contributions may also be appropriate towards costs incurred by a CSP which needs to update its systems to maintain, or make more efficient, its disclosure process.

11.4 Any CSP seeking to recover appropriate contributions towards its costs should make available to the requesting agency such information as they require, in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the CSP.

11.5 As costs are reimbursed from public funds, CSPs should take into account value for money when procuring, operating and maintaining the infrastructure required to comply with a notice. As changes to business systems may necessitate changes to systems put in place to comply with a warrant, CSPs should take this into account when making any changes to business systems.

11.6 Any CSP that has claimed contributions towards costs may be required to undergo an audit to ensure that a CSP has incurred expenditure for the stated purpose before those contributions are made. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

Costs in relation to a technical capability notice

11.7 CSPs that are subject to a technical capability notice under Part 9 of the Act are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a technical capability notice and the Act.

11.8 Any contribution towards these costs must be agreed by the Government before work is commenced by a CSP and will be subject to the Government considering, and agreeing, the technical capability proposed by the CSP.

11.9 Costs that may be recovered could include those related to the procurement or design of systems required to acquire communications data, their testing, implementation, continued operation and, where appropriate, sanitisation and decommissioning. Certain overheads may be covered if they relate directly to costs incurred by CSPs in complying with their obligations outlined above. This is particularly relevant for CSPs that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems. However, where a CSP expands or changes its network for commercial reasons, it is expected to meet any capital costs that arise.

Power to develop compliance systems

11.10 In certain circumstances it may be more economical for products to be developed centrally rather than CSPs creating multiple different systems to achieve the same end. Where multiple different systems exist it can lead to increased complexity, delays and cost in updating systems (such as for security updates).

11.11 Section 226 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop systems to support the disclosure of BCD. Such systems could operate in respect of multiple powers under the Act.

11.12 Where such systems are developed for use in CSPs the Secretary of State or agency will work closely with CSPs to develop systems which can be properly integrated into their networks. CSPs using such systems will have full sight of any processing of their data carried out by such systems. The Home Office should consult the Commissioner where relevant.

12 Oversight

12.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner, whose remit is to provide oversight of the use of the powers contained within Chapter 2 of part 6 of the Act. By statute the Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others qualified to assist the Commissioner in his or her work.

12.2 The Investigatory Powers Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law and this code by inspecting agencies and investigating any issue which they believe warrants further independent scrutiny. The Commissioner may undertake these inspections, as far as they relate to the Commissioner's statutory functions, entirely on his or her own initiative or the Commissioner may be asked to investigate a specific issue by the Prime Minister

12.3 The Commissioner will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the Commissioner must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers must, by law, offer all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

12.4 The Commissioner must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the national interest. Only the Prime Minister will be able to authorise redactions to the Commissioner's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

12.5 The Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publically available subject to public interest considerations. Public authorities and telecommunications operators may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce guidance for public authorities on how to apply and use Investigatory Powers. Wherever possible this guidance will be published in the interests of public transparency.

12.6 Anyone working for a public authority or communications service provider who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner, who will consider them. In particular, any person who exercises the powers described in the Act whose activities are covered by this code must report to the Commissioner any action undertaken which they believe to be contrary to the spirit or provisions of this code. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority. The Commissioner may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the Investigatory Powers Tribunal (IPT).

12.7 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to an individual who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the individual affected. Further information on errors can be found in chapter 10 of this code. The agency who has committed the error will be able to make representations to the Commissioner before they make their decision on whether it is in the public interest for the individual to be informed.

12.8 The Commissioner must also inform the affected individual of their right to apply to the Investigatory Powers Tribunal (see Complaints section for more information on the Investigatory Powers Tribunal) who will be able to fully investigate the error and decide if a remedy is appropriate.

12.9 Further information about the Investigatory Powers Commissioner, their office and their work may be found at:

13 Contacts / Complaints

General enquiries relating to bulk acquisition

13.1 The Home Office is responsible for policy and legislation regarding bulk acquisition of communications data under chapter 2 of Part 6 of the Act. Any queries should be raised by contacting:

Communications Data Policy Team
Home Office
2 Marsham Street
London
SW1P 4DF

commsdata@homeoffice.x.gsi.gov.uk

Complaints

13.2 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against public authority use of investigatory powers and human rights claims against the security and intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

13.3 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination.

13.4 This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: http://www.ipt-uk.com. Alternatively information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

13.5 If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

This code of practice relates to the powers and duties conferred or imposed under Chapter 2 of Part 6 of the Investigatory Powers Act relating to the acquisition of communications data in bulk by the security and intelligence agencies.

It provides guidance on:

- procedures to be followed for the acquisition of communications data in bulk;
- procedures to be followed for the storage, handling and selection for examination of communications obtained in bulk;
- keeping of records, including records of errors; and
- the oversight arrangements in place for acquisition and selection for examination of communications data obtained in bulk.

This code is aimed at members of the security and intelligence agencies who are involved in the acquisition of communications data in bulk and its storage, handling and selection for examination. It is also aimed at communications service providers' staff involved in the lawful disclosure of communications data under the Act.