Home Office

Bulk Acquisition of Communications Data

DRAFT Code of Practice

February 2017

Bulk Acquisition

DRAFT Code of Practice

Pursuant to Schedule 7 to the Investigatory Powers Act 2016

February 2017

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

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

Contents

1 Introduction

1.1 This code of practice relates to the powers and duties conferred or imposed under Chapter 2 of Part 6 of the Investigatory Powers Act 2016 ('the Act').

1.2 A bulk acquisition warrant under that Chapter 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 telecommunications operator, as well as to select for examination 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.

1.4 This code applies to the security and intelligence agencies ('SIAs') and communications service providers[1] ('CSPs') who have been issued with a warrant under Chapter 2 of Part 6.

1.5 This code is intended for use by the SIAs and by CSPs involved in the obtaining and disclosure of bulk communications data to the SIAs 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') 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 227 of the Act and by the Judicial Commissioners and inspectors who support the Commissioner.

1.8 The Home Office may issue further advice directly to the SIAs and CSPs as necessary.

1.9 For the avoidance of doubt, the duty to have regard to the code when exercising functions to which the code relates exists regardless of any contrary content of a SIA's internal advice or guidance.

[1] See paragraph 2.1

2 Definitions

Communications service provider

2.1 Communications service provider ('CSP') is not a term used in the Act, but is used generally to refer to a telecommunications or postal operator. The obligations under Chapter 2 of Part 6 of the Act apply to telecommunications operators only, so throughout this code, CSP refers only to a telecommunications operator.

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. This definition ensures that enforceable obligations in the Part of the Act to which this code applies 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 261(11) of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the telecommunication service provider); and section 261(13) defines 'telecommunication system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy. The definitions of 'telecommunications service' and 'telecommunication system' in the Act are intentionally broad so that they remain 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 telecommunication 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 telecommunications service. For example, an online market place may be a telecommunications operator if it provides a connection to an application/website. It may also be a telecommunications operator if and in so far as it provides a messaging service.

Composition of communications

2.6 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 261(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, 5 and 6 of the Act.

2.7 Communications data is a subset of systems data. Section 261(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 261(6)(b), be content, cannot be communications data.

Communications data

2.8 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[2].

2.9 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[3], of the communication.

2.10 Communications data in relation to telecommunication services can include 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.

2.11 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services.

2.12 Communications data about postal services cannot be acquired using a warrant issued under Chapter 2 of Part 6 of the Act.

2.13 In the context of telecommunications, communications data includes data held or obtainable by a CSP or which is available directly from a telecommunications system and comprises four elements, set out below.

---

[2] See paragraph 2.24 for the definition of content.

[3] As set out at section 261(6)(a).

Data about an entity to which a telecommunications service is provided and which relates to the provision of the service

2.14 This data 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.

2.15 An entity (see below for further details) can also include devices so this data 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.

2.16 Importantly, this data 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.

2.17 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.

Data 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

2.18 This data includes any information that is necessary to get a communication from its source to its destination, such as a 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.

2.19 This element of the communications data definition also includes data held, or capable of being obtained, by the CSP which is logically associated with a communication for the purposes of the telecommunication system by which the communication is being, or may be, transmitted. In practice this means any data which is necessary to route or transmit a communication which the CSP holds or could obtain, for example from the network.

2.20 This might include, for example, domain name system (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).

Data which relates to the use of a service or system

2.21 This element includes other information held by a CSP about the use of the service such as billing information.

Data which is about the architecture of a telecommunication system.

2.22 The definition of communications data additionally includes data held by a CSP about the architecture of the telecommunication 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.

2.23 Chapter 2 of Part 6 does not apply to any conduct by a SIA to obtain publicly or commercially available communications data. A Part 3 authorisation is not mandatory to obtain reference data, 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 SIA seeking to obtain this data from a CSP where the CSP requires it.

Content

2.24 The content of a communication is defined in 261(6) of the Act as the data which reveals anything of what might be reasonably be considered to be the meaning (if any) of that communication.

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

2.26 When a communication is sent over the telecommunication system 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.

2.27 There are two exceptions to the definition of content set out in section 261(6). The first is any meaning that could be inferred from the fact of the communication. When a communication is sent, the simple fact of the communication may convey some meaning, e.g. it could provide a link between persons or between a person and a service. This exception makes clear that any communications data associated with the communication remains communications data and the fact that some meaning can be inferred from it does not make it content.

2.28 The second makes clear that systems data cannot be content. In practice this means that a SIA should first determine whether the data enables or otherwise facilitates the functioning of a system or service. If the answer to this is yes, then the data is systems data regardless of whether it may reveal anything of what might be reasonably considered to be the meaning (if any) of the communication[4].

Guidance on definitions

2.29 The Home Office may issue further guidance to CSPs or SIAs on how the definitions in the Act apply.

[4] See interception and equipment interference codes of practice for more information.

3 General information on bulk acquisition

3.1 Bulk acquisition warrants authorise both the obtaining of communications data in bulk from a CSP and the selection for examination of the data 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 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[5] 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 SIA. In addition, the volume of data which may potentially be acquired is reflected in the fact that bulk acquisition warrants must be granted by the Secretary of State and are subject to approval by a Judicial Commissioner. Once acquired in bulk, selection of data for examination is only permitted for operational purposes specified on the warrant.

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 authorise the obtaining and selection for examination of communications data in relation to individuals in the UK.

[5] See paragraphs 3.8-3.11

Necessity and proportionality

3.8 Obtaining and selecting for examination communications data acquired under a bulk acquisition warrant is likely to involve an interference with a person's rights under the European Convention on Human Rights (ECHR). This is only justifiable if the conduct is necessary for a legitimate purpose and proportionate to that purpose. The Act recognises this by first requiring that the Secretary of State considers that the warrant is necessary for one or more of the following statutory purposes set out in the Act:

- In the interests of national security;
- For the purpose of preventing or detecting serious crime. Serious crime is defined in section 263(1)[6] as crime where the offence is one for which a person who has reached the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain or is 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. The power to issue a bulk acquisition warrant for the purpose of safeguarding the economic well-being of the UK may only be exercised in circumstances where the information it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.

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

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

- whether what is sought to be achieved could reasonably be achieved by other less intrusive mean,
- the public interest in the integrity and security of telecommunication systems, and
- any other aspects of the public interest in the protection of privacy (including the obligation for a public authority to comply with the Human Rights Act).

[6] See Paragraph 6 of Schedule 2 of the Act.

Trade Unions

3.12 As set out in section 158, the fact that the communications data that would be obtained under the warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State (or the Scottish Ministers).

4 Issuing 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 158 of the Act, bulk acquisition warrants are only available to the security and intelligence agencies. In this chapter, reference to an 'application' for a warrant includes the application form and the draft warrant (including the draft instrument and any draft schedules). An application for a bulk 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 When completing a warrant application, the SIA must ensure that the case for the warrant is presented in the application in a fair and balanced way, including information which supports or weakens the case for the warrant.

4.4 Prior to submission, each application is subject to a review within the SIA 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). A bulk warrant must always be necessary in the interests of national security. The scrutiny of the application will 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 each of the operational purposes specified.

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

a) Background to the application;

b) Description of the communications data 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[7];

c) Description of the conduct to be authorised, which must be restricted to the obtaining of communications data, or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant;

d) The operational purposes for which the communications data obtained under the warrant may be selected for examination;

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

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

f) An explanation of why the acquisition of communications data in bulk 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;

g) A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, explaining why what is sought to be achieved could not reasonably be achieved by less intrusive means;

h) An assurance that the data 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 172 of the Act; and

i) An assurance that all data will be kept for no longer than necessary and handled in accordance with the safeguards required by section 171 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 giving effect to the warrant. CSPs are unlikely to receive a copy of the operational purposes specified in the warrant. The warrant should include the following:

a) a description of the communications data to be acquired;

b) the steps a CSP must take to give effect to the warrant;

c) a list of the operational purposes for which any communications data obtained under the warrant may be selected for;

d) the date the warrant was issued; and

e) the warrant reference number.

Authorisation of a bulk acquisition warrant

Necessity

4.7 Before a warrant under Chapter 2 of Part 6 of the Act can be issued, the Secretary of State must consider that the warrant is necessary for one or more of the statutory purposes, as set out at sections 158(1)(a) and 158(2). One of the statutory purposes must always be national security. If the Secretary of State is not satisfied that the warrant is necessary in the interests of national security, then it cannot be issued.

4.8 Before a bulk acquisition warrants can be issued, the Secretary of State must also consider that the selection for examination of data obtained under the warrant is necessary for one or more of the specified operational purposes (section 158(1)(c)). Setting out the operational purposes on the warrant limits the purposes for which data obtained under the warrant can be selected for examination.

4.9 When considering the specified operational purposes, the Secretary of State must also be satisfied that selection for examination of data obtained under the warrant is necessary for one or more of the statutory purposes set out on the warrant. 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, the selection for examination for each specified operational purpose on that warrant must be necessary for one or both of these two broader purposes. In cases where it is necessary and proportionate for the data to be made available to another of the security and intelligence agencies or an international partner, the operational purposes specified in the warrant may include operational purposes relating to that third party providing the tests in section 171 are met.

4.10 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 158(1)(a) or section 158(2) purpose, and which meets the conditions set out in section 172 is, in fact, selected for examination. The Investigatory Powers Commissioner is under a duty to review the adequacy of those arrangements.

Proportionality

4.11 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.

4.12 In considering whether a bulk acquisition warrant is necessary and proportionate, the Secretary of State must take into account whether what is sought to be achieved by the warrants could reasonably be achieved by other less intrusive means (section 2(2)(1) of the Act). For example, obtaining the required information through a less intrusive power such as the targeted acquisition of communications data, or the targeted acquisition of communications data using the request filter, which will provide an additional safeguard for such communications data.

Safeguards

4.13 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, retention and selection for examination of communications data obtained under the warrant. These safeguards are explained at chapters 6 and 9 below.

Judicial Commissioner approval

4.14 Before a bulk acquisition warrant can be issued, the Secretary of State's decision to issue it must be approved by a Judicial Commissioner. Section 159 of the Act sets out the test that a Judicial Commissioner must apply when considering whether to approve the decision. The Judicial Commissioner will review the Secretary of State's 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 will also review the Secretary of State's conclusions as to whether each of the operational purposes specified on the warrant is a purpose for which selection is, or may be, necessary.

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

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

4.17 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).

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

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

Duration of warrants

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

5 Renewals, modifications, and cancellation

Renewal of a bulk acquisition warrant

5.1 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 163 of the Act), with the approval of a Judicial Commissioner. Applications for renewals are 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 communications data 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 158(2), and why it is considered that obtaining of communications data in bulk continues to be proportionate.

5.2 In deciding to renew a bulk acquisition warrant, the Secretary of State must also consider that the selection for examination of communications data 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 158(1)(a) and 158(2)) on the warrant.

5.3 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 communications data in bulk, it is not necessary for the Secretary of State to consider that acquisition of communications data continues to be necessary before making a decision to renew the warrant.

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

5.5 In those circumstances where the assistance of CSPs has been sought, a copy of the warrant renewal instrument (or part of that warrant that is relevant to the particular CSP or other person) will be forwarded to all those on whom a copy of the original warrant instrument has been served, providing they are still actively assisting. A renewal instrument will include the reference number of the warrant or warrants being renewed under the instrument.

Modification of a bulk acquisition warrant

5.6 A bulk acquisition warrant may be modified at any time by an instrument issued by the person permitted to do so under the provisions at section 164 of the Act. A bulk acquisition warrant may be modified to add, vary or remove an operational purpose for which communications data obtained under the warrant may be selected for examination.

5.7 If a SIA requires a change to the communications described in the warrant or a change to the statutory purpose for which the warrant is issued, then an additional or replacement warrant must be sought. Nothing in section 164 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.

5.8 In circumstances where a modification is being made to add or vary an operational purpose, this is a **major modification** and it must be made by a Secretary of State and must be approved by a Judicial Commissioner before the modification comes into force. The Act permits that when it is not reasonably practicable for the Secretary of State to sign a major modification instrument, a delegate may sign it on their behalf. Typically, this scenario will arise where the Secretary of State is not physically available to sign the warrant because, for example, they are on a visit or in their constituency. The Secretary of State must still personally authorise the modification.

5.9 Once the modification comes into force, the added or varied operational purpose may be used to select for examination data from any communications data retained under that warrant, even if the communications data was acquired prior to the addition or variation of the operational purpose.

5.10 In circumstances where a bulk acquisition warrant is being modified to remove an operational purpose, this is a **minor modification** and 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, section 164(8) provides that they must modify the warrant to remove that operational purpose.

5.11 As set out above, a bulk acquisition warrant may authorise the acquisition of communications data in bulk and the selection for examination of the data collected under the warrant.

5.12 There will be limited circumstances where it may no longer be necessary, or possible, to continue the bulk acquisition of communications data, such as where the communications service provider providing assistance with giving effect to the warrant has ceased business. In such circumstances, it may continue to be necessary and proportionate to select for examination the data obtained under that warrant. The Act therefore provides that a bulk acquisition warrant can be modified such that it no longer authorises the acquisition of communications data in bulk, but continues to authorise selection for examination of data already obtained under the warrant.

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

5.14 In accordance with section 164(12), a SIA is permitted to amend a warrant as long as such an amendment does not alter the conduct that is authorised by the warrant. An example of this would be to correct a spelling.

Urgent modifications of a bulk acquisition warrant

5.15 In urgent cases a major modification adding or varying an operational purpose can be made by a Secretary of State. An example of an urgent case may be where a sudden terrorist incident requires the urgent selection for examination of the data already held for an operational purpose not listed on the warrant.

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

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

Warrant cancellation

5.18 The Secretary of State, or a senior official acting on their behalf, may cancel a bulk acquisition warrant at any time. Such a person 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 grounds of one of the statutory purposes 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 none of the operational purposes specified on the warrant remain necessary for the examination of communications data.

5.19 SIAs will therefore need to keep their warrants under regular 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.

5.20 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 existing CSPs who have given effect to the warrant during the preceding twelve months.

5.21 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.

5.22 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 Examination safeguards

6.1 Section 172 of the Act provides specific safeguards relating to the selection for examination of communications data obtained under a bulk acquisition warrant. Further guidance on these safeguards is provided in this Chapter.

6.2 Sections 172(1) and (2) make clear that selection for examination may only be carried out 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. Communications data selected for examination for an operational purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained for any of the authorised purposes.

6.3 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 161 of the Act makes clear that the heads of the SIAs must maintain a central list of all of the operational purposes which they consider are purposes for which communications data may be acquired in bulk and 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.

6.4 The central list of operational purposes will not be limited to operational purposes relevant to bulk acquisition 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.

6.5 Section 161 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.

6.6 Section 158 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 161 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 acquired data may only be selected for examination for specific reasons.

6.7 Section 164 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 modification is categorised as a major modification and must be made by the Secretary of State and approved by a Judicial Commissioner before the modification may take effect. In such circumstances, the provisions at section 164 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.

6.8 The Act therefore creates a strict approval process in circumstances where a SIA 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.

6.9 In addition to the central list of operational purposes having to be approved by the Secretary of State, section 161 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 of Parliament.

6.10 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. Other than in exceptional circumstances, it will always be necessary for a bulk acquisition warrant to require the full range of operational purposes relevant to the SIA's statutory functions (and, where appropriate, relevant to the statutory functions of the other two SIAs) to be specified in relation to the selection for examination of data obtained under the warrant.

6.11 The analysis of communications data obtained in bulk is a primary means by which the security and intelligence agencies are able to discover and assess threats to the United Kingdom. This can only be achieved effectively through the aggregation of data from a wide range of sources acquired and retained under multiple bulk warrants, not limited to communications data acquired in bulk. Such analysis allows the SIAs to draw together fragments of information into coherent patterns, which allow for the identification of those threats while at the same time minimising intrusion into privacy.

6.12 As well as being necessary for one of the operational purposes, any selection for examination of communications data must be necessary and proportionate.

6.13 No data may be selected for examination other than in accordance with specified operational purposes. In general, automated systems should, where possible, be used to effect the selection for examination in accordance with section 172 of the Act and the specified operational purposes.

6.14 A limited number of officials may also be permitted to access the system during the processes of processing and selection for examination, for example to check system health. Such access must itself be necessary on the grounds specified in sections 158(1)(a) and 158(2). Where such access involves selection for examination of data, it must be necessary and proportionate for an operational purpose specified on the warrant. SIA arrangements for access will be kept under review by the Investigatory Powers Commissioner during his or her inspections.

6.15 No data may be selected for examination for the specified operational purposes unless this is necessary and proportionate in all the circumstances. In addition, arrangements must be put in place to provide for the creation and retention (for the purposes of subsequent examination or audit) of documentation[8] outlining why access to the data by authorised persons is necessary and proportionate, and the applicable operational purposes.

6.16 Periodic audits should be carried out to ensure that the requirements set out in section 171 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 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.

6.17 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 use of operational purposes on bulk acquisition warrants.

6.18 Section 171 provides for the giving of any communications data acquired under a bulk acquisition warrant, or a copy of any such data, to any overseas authorities. For this to happen, the Secretary of State must first ensure that the overseas authority has in place retention, disclosure and examination safeguards corresponding to those specified in the Act, to the extent the Secretary of State considers appropriate.

[8] Any such documentation should be made available to the Commissioner on request for the purposes of oversight

Selection for examination of data relating to those in certain professions

6.19 The fact a communication took place does not disclose what was discussed, considered or advised.

6.20 However, the degree of interference with an individual's rights and freedoms may be higher where communications data 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, 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.

6.21 Section 2 of the Act makes clear that due regard must be given to whether the level of protection applied in relation to the acquisition of communications data in bulk is higher because of the particular sensitivity of that information. Examples of sensitive information include but are not restricted to legally privileged information, confidential journalistic material, the identity of a journalist's source, and communications between a Member of Parliament and their constituent.

6.22 Such situations do not preclude selecting the data for examination. However officers, 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.

6.23 The nature of bulk data means that in many cases, the authorised person will not know who the communications data relates to at the point of its selection for examination. However, authorised persons must consider any additional sensitivities in all cases where it is intended or known that the data being selected for examination includes communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion.

Selection for examination to determine the source of journalistic information

6.24 Issues surrounding the infringement of the right to freedom of expression may arise if communications data is selected for examination for the purpose of identifying the communications data of an identified or suspected journalist, an identified source or a suspected source of journalistic information and particularly, but not solely, where it is done for the purpose of identifying or confirming the identity or role of an individual as a journalist's source.

6.25 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 communications data is selected for examination in order to determine the source of journalistic information, there must therefore be an overriding requirement in the public interest.

6.26 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, any reference to sources should be understood to include any person acting as an intermediary between a journalist and a source.

6.27 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 personal rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest.

6.28 In the exceptional event that an officer were to select for examination communications data 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, other than for the purposes of destruction, as a result of such selection for examination must be reported to the Investigatory Powers Commissioner at the next inspection.

6.29 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.

6.30 The requirement for senior approval does not apply where the intent is to examine communications data obtained in bulk 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).

6.31 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.

Offence of breaching examination safeguards

6.32 Data obtained under a bulk acquisition warrant may only be selected for examination subject to the safeguards in section 172 of the Act. Section 173 of the Act makes it an offence for a person deliberately to select data for examination in breach of these safeguards where that person knows or believes such selection does not comply with the safeguards.

7 Implementation of warrants and CSP compliance

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

7.2 Section 168 of the Act then allows the SIA to require the disclosure of communications data acquired under the bulk warrant, or to require the assistance of other persons in giving effect to the warrant. Section 168 makes clear that the warrant may be served on any person, inside or outside the UK, who may be able to provide such assistance in relation to that warrant.

7.3 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 the person by or on behalf of the SIA. This applies to any company offering or providing services to persons in the UK, irrespective of where the company is based.

7.4 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, or any other means, are reasonably practicable). The implementing authority must take steps to bring the contents of the warrant to the attention of the relevant person.

7.5 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

7.6 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. The Act places a requirement on CSPs to take all such steps for giving effect to the warrant as are notified to them. The steps which may be required of CSPs are limited to those which it is reasonably practicable to take. The duty to comply with a warrant applies only to a person who is capable of complying with it. Where a technical capability notice is in place and consideration is being given to a provider's compliance with the duty, the steps which it is reasonably practicable for the provider to take will include every step it would have been reasonably practicable for the provider to take if the provider had complied with all of the obligations in the notice. Knowingly failing to comply is an offence which, on summary conviction in the UK, may result in imprisonment and/or a fine.

7.7 The steps which may be required are limited to those which it is reasonably practicable to take (section 170(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.

7.8 A copy of the warrant must be served in such a way as to bring the contents of the warrant to the attention of the person or CSP who the SIA considers can provide assistance in relation to it. The SIA may provide the following to the person or 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 of the schedules contained in the warrant with the omission of the remainder of the warrant. Warrants must specify the communications data to be obtained and the operational purposes for which any data obtained under the warrant may be selected for examination, but CSPs are unlikely to 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 to notify the CSP of steps they are required to take to give effect to the warrant 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 either be provided in this covering document or will be available in the handbook provided to all CSPs require to provide communications data in bulk.

Offence of unauthorised disclosure

7.9 A CSP served with a bulk acquisition warrant must keep the warrant secret, as required by section 174 of the Act. The offence of unauthorised disclosure occurs when any CSP, or employee of a CSP, reveals the content or existence of a warrant without reasonable excuse.

7.10 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.

Maintenance of a technical capability

7.11 CSPs may be required under section 253 of the Act to provide a technical capability to give effect to bulk acquisition warrants and notices or authorisations for the acquisition of communications data. The purpose of maintaining a technical capability is to ensure that, when a warrant, authorisation or notice is served, companies can give effect to it securely and quickly. Small companies (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.

7.12 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. The Secretary of State may only give a notice where the decision to do so has been approved by a Judicial Commissioner. In practice, technical capability notices will only be given to communications service providers that are likely to be required to give effect to warrants, authorisations or notices given on a recurrent basis.

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

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

- obligations to provide facilities or services of a specified description;
- obligations relating to apparatus owned or operated by a relevant operator;
- obligations relating to the removal of electronic protection applied, by or on behalf of the relevant operator on whom the obligation has been placed, to any data;
- obligations relating to the security of any postal or telecommunications services provided by the relevant operator (so far as they relate to the capability required by the technical capability notice); and
- obligations relating to the handling or disclosure of any material or data.

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

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

7.17 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 is able to give effect to the notice and on whom it is reasonably practicable to impose these requirements. It is possible that more than one CSP will be involved in the provision of the capability, particularly if more than one CSP applies electronic protections to the relevant data.

7.18 While an obligation to remove encryption may only relate to protections applied by or on behalf of the company on whom the obligation is placed, a warrant may require a CSP to take such steps as are reasonably practicable to take to give effect to it. This will include, where applicable, providing communications or data in an intelligible form. An example of such circumstances might be where a CSP removes encryption from communications or data for their own business reasons.

Consultation with service providers

7.19 Before giving a notice, the Secretary of State must consult the CSP. In practice, informal consultation is likely to take place long before a notice is given. The Government will engage at the outset 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.

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

Matters to be considered by the Secretary of State

7.21 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 and its effect on the CSP. 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.

7.22 As part of the decision the Secretary of State must take into account, amongst other factors, the matters specified in section 255(3):

- the likely benefits of the notice – this may take into account projected as well as existing benefits;
- the likely number of users (if known) of any telecommunications service to which the notice relates – this will help the Secretary of State to consider both the necessity of the capability but also the likely benefits;
- the technical feasibility of complying with the notice – taking into account any representations made by the communications service provider;
- 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.

7.23 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 have regard to the following when giving, varying or revoking a notice so far as they are relevant:

- whether what is sought to be achieved by the 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.

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

7.25 Before the notice may be given, a Judicial Commissioner must approve the Secretary of State's decision to give the notice. In deciding whether to approve the Secretary of State's decision to give a relevant notice, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the notice is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. In reviewing these conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. In addition, the Judicial Commissioner must review the conclusions with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

Giving a notice

7.26 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.

7.27 Section 255(6) provides that technical capability notices may be given to, and obligations may be imposed on, CSPs 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.

7.28 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 bulk acquisition of communications data.

7.29 As set out in section 253(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.

7.30 The notice will also specify the telecommunications system or systems to which the obligations will apply.

7.31 A person to whom a technical capability notice is given is under a duty to comply with the notice. In respect of a technical capability notice relating to equipment interference or bulk acquisition warrants, the duty to comply with a technical capability notice is enforceable against a person in the UK by civil proceedings by the Secretary of State. The duty to comply with a technical capability notice relating to targeted or bulk 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

7.32 The Government does not publish or release identities of those subject to a technical capability notice, as to do so may identify operational capabilities or harm the commercial interests of companies that have been given a notice. Should criminals become aware of the capabilities of the SIAs, they may alter their behaviours and change CSP, making it more difficult to detect their activities of concern.

7.33 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[9].

7.34 Section 255(8) of the Act provides for the person to disclose the existence and contents of a technical capability notice with the permission of the Secretary of State. Such circumstances might include disclosure:

- to a person (such as a system provider) who is working with the CSP to give effect to the notice;
- to relevant oversight bodies;
- to a legal advisor in contemplation of legal proceedings, or for the purpose of those proceedings;
- to regulators in exceptional circumstances where information relating to a capability may be relevant to their enquiries;
- to other 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

7.35 Section 256(2) of the Act imposes an obligation on the Secretary of State to keep technical capability notices under regular review. This helps to ensure that the notice itself, or any of the requirements or restrictions imposed by it, remains necessary and proportionate. This evaluation differs from the process provided for in section 257 of the Act, which permits communications service providers to request a review of the requirements placed on them in a technical capability notice should they consider these to be unreasonable.

7.36 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.

[9] See section 255(8)

7.37 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.

7.38 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.

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

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

Variation of technical capability notices

7.41 The communications market is constantly evolving and CSPs subject to technical capability notices will often launch new services.

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

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

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

7.45 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 7.35); or
- to amend or enhance the security requirements.

7.46 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, must consider whether the existing notice should be varied.

7.47 Before varying a notice, the Secretary of State must consult the CSP to understand the impact of the change and must take into account the same factors as when deciding to give a notice, including cost and technical implications. The Government should also consult the SIAs to understand the operational impact of any change to the notice.

7.48 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above.

7.49 Once a variation has been agreed by the Secretary of State and the decision to vary a notice has, where necessary, been approved by a Judicial Commissioner, arrangements will be made for the 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

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

7.51 Circumstances where it may be necessary 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.

7.52 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

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

7.54 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.

7.55 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 TAB 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.

7.56 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 Secretary of State.

7.57 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 communications service provider to comply with the notice so far as referred. Notwithstanding the review, the CSP may be required to provide assistance in giving effect to a warrant or authorisation.

8 Costs

Making of contributions

8.1 Section 249 of the Act recognises that CSPs incur costs in complying with requirements in the Act, including warrants under Chapter 2 of Part 6 of the Act and technical capability notices to maintain technical capabilities under Part 9. The Act, therefore, requires the Secretary of State to have in place arrangements to ensure that providers receive an appropriate contribution to these costs.

8.2 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 SIAs' necessary and proportionate requirement for the acquisition of communications data in bulk in support of their investigations and operations to protect the public. The provision of public funding may be subject to terms and conditions determined by the Secretary of State.

8.3 It is legitimate for a CSP to seek contributions towards its costs which may include an element of funding towards those general business overheads required in order to facilitate the timely disclosure of the communications data specified in the 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, certain staff benefits or arrangements made in line with the terms and conditions of employment, such as bonuses paid to members of staff that are reflective or representative of the company's performance, will be excluded from this category of costs. Such matters are arranged between the employer and employee and the Government does not accept responsibility for such costs.

8.4 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, certain staff benefits or arrangements made in line with the terms and conditions of employment, such as bonuses paid to members of staff that are reflective or representative of the company's performance, will be excluded from this category of costs. Such matters are arranged between the employer and employee and the Government does not accept responsibility for such costs.

8.5 It may also be appropriate for the Government to contribute towards costs incurred by a CSP to update its systems to maintain, or make more efficient, its bulk acquisition 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 bulk acquisition of communications data.

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

8.7 Any CSP that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made by the Secretary of State. This is to ensure that expenditure has 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

8.8 In certain circumstances it may be more economical for apparatus, systems or other facilities or services required to enable or facilitate CSPs to comply with obligations under the Act to be developed centrally rather than 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).

8.9 Section 250 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop systems to support the disclosure of communications data in bulk. Such systems could operate in respect of multiple powers under the Act.

8.10 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.

9 General safeguards

9.1 All communications data acquired under the authority of a bulk acquisition warrant 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 171 of the Act. Breaches of these safeguards must be reported to the Investigatory Powers Commissioner in a fashion agreed with him or her. The SIAs 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 Section 171 of the Act requires that disclosure, copying and retention of data obtained under the warrant is limited to the minimum necessary for the authorised purposes. Section 171(3) of the Act provides that something is necessary for the authorised purposes if it:

- is, or is likely to become, necessary in the interests of national security or on any other purposes falling within section 158(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[10];
- 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 1967 or the Public Records Act (Northern Ireland) 1923.

Personnel security

9.3 All persons who may have access to communications data obtained in bulk or need to see any reporting in relation to it must be appropriately security cleared. On an annual basis, managers must identify any concerns that may lead to the security clearance of individual members of staff being reconsidered. The security clearance of each individual member of staff must also be periodically reviewed. Where it is necessary for one SIA to disclose data to another, it is the former's responsibility to ensure that the recipient has the necessary security clearance.

[10] Communications data obtained for one purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained for another.

Dissemination of communications data obtained in bulk

9.4 Communications data obtained in bulk, and more typically the intelligence derived from it, will need to be disseminated both within and between SIAs, as well as to consumers of intelligence (which includes oversight bodies, Secretary of State, etc.), where necessary in order for action to be taken on it. The number of persons to whom any of the data is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out in section 171(2) of the Act. This obligation applies equally to disclosure to additional persons within a SIA, and to disclosure outside the agency.

9.5 It is enforced by prohibiting disclosure to persons who have not been appropriately security cleared and also by the need-to-know principle: communications data acquired in bulk 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 data to carry out those duties. In the same way, only so much of the data may be disclosed as the recipient needs.

9.6 The obligations apply not just to the originally acquiring SIA 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 originally acquiring agency's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

9.7 Section 171(9) of the Act stipulates that where communications data obtained under a bulk acquisition warrant is disclosed to the authorities of a country or territory outside the UK, the Secretary of State must ensure arrangements are in force so that data is only handed over to overseas authorities if the following requirements are met:

- it appears to the Secretary of State that requirements corresponding to the requirements in 171(2) and 171(5) (relating to minimising the extent to which data is disclosed, copied, distributed and retained other than for the purposes of destruction) will apply to the extent, if any, that he or she considers appropriate; and

- where unselected data obtained under a bulk warrant is disclosed to overseas authorities, it appears to the Secretary of State that requirements corresponding to the requirements of section 172 (safeguards relating to the examination of data) will also apply to the extent, if any, that the Secretary of State considers appropriate.

Copying

9.8 Communications data obtained under a bulk acquisition warrant may only be copied to the extent necessary for the authorised purposes set out in section 171(3) of the Act. This includes direct copies of data, in whole or in part, which identify the material as having been obtained under a warrant, and any record referring to a bulk acquisition warrant and which is a record of the identities of the persons to or by whom the material was sent or to whom the material relates.

Storage and transfer of data

9.9 All copies, extracts and summaries of communications data obtained under a bulk acquisition warrant must be handled and stored securely, so as to minimise the risk of loss or theft. In particular they must be held so as to be inaccessible to persons without the required level of security clearance. This requirement 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.

9.10 In particular, each SIA 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 clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

9.11 Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies, extracts and summaries of it held within the SIA must be scheduled for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes. In this context, destroying material means taking such steps as might be necessary to make selection for examination unavailable to analysts or investigators pending deletion. If communications data is retained other than for the purposes of destruction, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 171(3) of the Act.

Acquisition Offence

9.12 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.

9.13 The roles and responsibilities laid down are designed to prevent the 'knowing or reckless' acquisition of communications by a public authority[11] 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 this code, will mitigate the risk of any offence being committed.

9.14 It is a defence if the person who obtained the communications data can show that they acted in the reasonable belief that they had lawful authority to obtain that data.

9.15 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.

9.16 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.

[11] The offence applies only to those public authorities listed in Schedule 4 and local authorities

10 Record keeping and error reporting

Records

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

- All applications made for bulk acquisition warrants, and applications made for the renewal of such warrants or modifications to those warrants;
- All warrants, associated schedules, renewal instruments and copies modification instruments (if any);
- Where any application is refused, the grounds for refusal as given by the Secretary of State or Judicial Commissioner;
- In relation to each warrant, the dates on which collection of communications data started and stopped.

10.2 Records should also be kept of the arrangements for securing that data has only been selected for examination for the specified operational purposes. Records should be kept of the arrangements by which the requirements of section 171(2) (minimisation of copying and distribution of bulk communications data), section 171(5) (destruction of bulk communications data) and section 172 (examination of bulk communications data) are to be met.

10.3 The Secretary of State must keep records of the warrant authorisation process. This should include:

- All advice provided to the Secretary of State to support his/her consideration as to whether to issue or renew the 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.
- A record of whether, following refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner.
- Where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given

10.4 Each relevant 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 decisions to issue a bulk acquisition warrant that a Judicial Commissioner refused to approve.
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse to approve the decision to issue a bulk acquisition warrant.
- The number of decisions to issue a bulk acquisition warrant that were refused by the Investigatory Powers Commissioner, following a referral from the Secretary of State.
- 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 the Secretary of State or Judicial Commissioner refused to approve the renewal of.
- The number of bulk acquisition warrants that were cancelled.
- The number of bulk acquisition warrants extant at the end of the year.

10.5 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 158(1)(a) and section 158(2) purpose(s) specified on the warrant.
- The operational purposes specified on the warrant.
- The details of modifications made to add, vary or remove an operational purpose from the warrant.
- The number of modifications made to add or vary an operational purpose that were made on an urgent basis.
- The number of modifications made to add or vary an operational purpose (including on an urgent basis) that a Judicial Commissioner refused to approve.
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse to approve the decision to modify a bulk acquisition warrant.

10.6 These records must be sent in written or electronic form to the Investigatory Powers Commissioner, as requested by the Commissioner. Guidance on record keeping may be issued by the Investigatory Powers Commissioner. Guidance may also be sought from the Commissioner by agencies.

Errors

10.7 This section provides information regarding errors. Proper application of the Investigatory Powers Act 2016 and thorough procedures for operating its provisions, including for example the careful preparation and checking of warrants, modifications and schedules, should reduce the scope for making errors whether by a public authority, CSP or other persons assisting in giving effect to a warrant.

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

10.9 Section 231(9) of the Act sets out what is meant by a "relevant error", and section 235(6) requires that any relevant error of which a public authority or CSP is aware must be reported to the Commissioner.

10.10 Section 231(9)(a) makes clear that an error can only be a relevant error where it is one that has been made by a public authority in complying with any requirements imposed by the Act (or any other enactment), which are subject to review by the Investigatory Powers Commissioner. Section 231(9)(b) sets out that a relevant error must also be one of a description outlined in a Code of Practice under Schedule 7 of the Act. In relation to bulk acquisition, a relevant error is one that meets the description at 10.12 below.

10.11 An error can only occur after the acquisition of data has been initiated.

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

- The bulk acquisition of communications data without lawful authority has occurred and communications data acquired in bulk has been diverted or recorded so as to be made available to a person subsequently[12];
- There has been a failure to adhere to the safeguards set out at sections 171 and 172 of the Act.

10.13 The following provides a list of possible relevant errors by a SIA in complying with the requirements imposed on it that would fall within the descriptions provided above:

- human error, such as incorrect transposition of information which leads to the wrong communications data being acquired; or

[12] For the purposes of this section, bulk acquisition without lawful authority is a failure for a public authority to have in place lawful authority to conduct bulk acquisition, in accordance with section 158 of the Act, and where the exercise of that acquisition, were it lawfully authorised, would be a matter which the Investigatory Powers Commissioner would have oversight of under section 229 of the Act.

- failure to cease bulk acquisition when the bulk acquisition warrant has been cancelled;
- a breach of the relevant safeguard section caused by software or hardware issues;
- selection for examination without a valid operational purpose;
- retention of data when it is no longer necessary for the authorised purposes.

10.14 The description of the relevant errors above captures those circumstances where an error will involve an interference with privacy. Such errors can have very significant consequences on an affected individual's rights and that is why the Act requires that all relevant errors must be reported to the Commissioner by the SIA or CSP that is aware of the error.

10.15 When an error has occurred, the SIA that made the error must notify the Commissioner as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance process 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.

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

10.17 Section 235(6) of the Act also places a requirement on CSPs to report to the Commissioner any relevant error, committed by a public authority, of which they become aware. In such circumstances, the process for reporting the error to the Commissioner at paragraphs 10.15 and 10.16 above applies to CSPs as it applied to the SIAs. In addition, the CSP should inform the SIA as soon as they become aware that SIA may have made an error. The CSP may then work in conjunction with the SIA to confirm the fact of the error and report it to the Commissioner.

10.18 A full report must be sent to the Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days of establishing the fact of the error, the reasons this is the case. Where the report is being made by the SIA that made the error, that report should also include: the cause of the error; the amount of data obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether the data has been retained other than for the purposes of destruction or destroyed; and a summary of the steps taken to prevent recurrence.

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

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

10.21 If a SIA discovers a CSP error (which cannot therefore be a relevant error) they should notify 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.

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

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 may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal (see section 11).

10.24 Section 231 of the Act states that the Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

10.25 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 his or her decision, the Commissioner must require the SIA 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 Oversight

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

11.2 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. Section 236 also provides for the Intelligence and Security Committee of Parliament to refer a matter to the Commissioner with a view to carrying out an investigation, inspection or audit.

11.3 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.

11.4 Anyone working for a SIA or CSP 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 this chapter, 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 SIA. 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).

11.5 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 SIA 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.

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

11.7 The Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publically available subject to public interest considerations. SIAs and CSPs 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.

11.8 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: [insert website]

12 Contacts / Complaints

General enquiries relating to bulk acquisition

12.1 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

12.2 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.

12.3 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.

12.4 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: 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

12.5 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 data 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.