Home Office

Bulk Acquisition

DRAFT Code of Practice

Autumn 2016

Bulk Acquisition

DRAFT Code of Practice

Published for consultation alongside the Investigatory Powers Bill

Autumn 2016

Contents

1 Introduction

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

1.2 A bulk acquisition warrant under that Part is a warrant which authorises or requires the person to whom it is addressed to obtain the communications data described in the warrant from a communications service provider (CSP), as well as to access the acquired communications data, as specified in the warrant.

1.3 Throughout this code the data acquired under a bulk acquisition warrant is referred to as bulk communications data ('BCD').

1.4 This code applies to the Security and Intelligence Agencies ('SIA') and communications service providers[1] who have been issued with a warrant under Part 6, Chapter 2.

1.5 This code should be readily available to members of the SIA involved in the acquisition of communications data in bulk and its examination, and to CSPs involved in the disclosure of this data to a member of the SIA under the Act. The Act provides that persons exercising any functions to which this code relates must have regard to the code. Although failure to comply with the code does not, of itself, make a person liable to criminal or civil proceedings.

1.6 The Act provides that the code is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to a question before any court or tribunal hearing any such proceedings, or to the Investigatory Powers Tribunal (the 'IPT') or to the Investigatory Powers Commissioner ('the Commissioner') or the Information Commissioner when overseeing the powers conferred by the Act, it may be taken into account.

1.7 The exercise of powers and duties under Chapter 2 of Part 6 of the Act and this code are kept under review by the Investigatory Powers Commissioner appointed under section 205 of the Act and by his Judicial Commissioners and inspectors who work from the Investigatory Powers Commission (the 'IPC').

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

1.9 This code extends to the United Kingdom[2].

1.10 For the avoidance of doubt, the guidance in this code takes precedence over any contrary content of a public authority's internal advice or guidance.

---

[1] See paragraph 2.1

[2] This code and the provisions in Parts 3 and 4 of the Act do not extend to the Crown Dependencies and British Overseas Territories.

2 Scope and definitions

Communications service provider

2.1 The obligations under Parts 3 and 4 of the Act apply to telecommunications operators and postal operators. Throughout this code, communications service provider ('CSP') is used to refer to a telecommunications operator or postal operator. CSP is not a term used in the Act.

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

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

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

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

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

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

Composition of communications

2.8 For the purposes of the Act communications may comprise two broad categories of data: systems data and content. Some communications may consist entirely of systems data. Section 237(6)(b) makes clear that anything which is systems data is, by definition, not content. When permitted by the Act, certain data may also be separated from the remainder of a communication in circumstances where, if it were so separated, it would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication. This is identifying data. Systems data and identifying data may be obtained by interception or equipment interference warrants under Parts 2 and 5, and 6 of the Act. Further details on systems and identifying data can be found in the interception and equipment interference codes of practice.

2.9 Communications data is a subset of systems data. Section 237(5) is clear that, even though systems data cannot be content, communications data is limited to data which does not reveal anything of what might reasonably be considered to be the meaning of the communication, excepting any meaning arising from the fact of the communication or transmission of the communication. That is, any systems data which would, in the absence of section 237(6)(b), be content, cannot be communications data.

2.10 Any communications data obtained as part of systems data under an interception warrant is intercept material. Any such data must be treated in accordance with the restrictions on the use of intercept material in the Interception Code of Practice. Communications data obtained as part of systems data under an equipment interference warrant must be handled in accordance with the safeguards set out in the Equipment Interference Code of Practice.

Communications data

2.11 The term ‘communications data’ includes the ‘who’, ‘when’, ‘where’, and ‘how’ of a communication but not the content i.e. what was said or written[3].

2.12 It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning[4], of the communication.

---

[3] See paragraph 2.26 for the definition of content.

[4] As set out at section 237(6)(a).

2.13 It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

2.14 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services – i.e. postal services or telecommunications services.

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

2.16 Communications data in relation to telecommunications operators' services and systems includes data held or obtainable by a CSP or which is available directly from a telecommunications system and which:

- is about an entity to which a telecommunication service is provided **and** relates to the provision of the service;
- is comprised in, included as part of, attached to or logically associated with a communication for the purposes of a telecommunication system that facilitates the transmission of that communication; or
- relates to the use of a service or system; or
- is about the architecture of a telecommunication system.

2.17 The first limb of the definition includes information about any person to whom a service is provided, whether a subscriber or guest user and whether or not they have ever used that service. For example this may include information about the person associated with an email address even if that email address has not been used since its creation.

2.18 An entity can also include devices so this limb would cover information about the devices owned by a customer as well as the services to which the owner of the devices subscribes. This data may include names and addresses of subscribers.

2.19 Importantly this limb is limited to data held or obtained by the CSP in relation to the provision of a telecommunications service – it does not include data which may be held about a customer by a CSP more generally which are not related to the provision of a telecommunications service. For example, for a social media provider data such as the status of the account, contact details for the customer and the date a person registered with the service would all be communications data as they relate to the use of the service. However, other data held by the provider about a customer which does not relate to the provision of the telecommunication service, including personal information such as political or religious interests included in profile information, is not within scope of the definition of communications data.

2.20 The second limb includes any information that is necessary to get a communication from its source to its destination, such as dialled telephone number or internet protocol (IP) address. It includes data which:

- identifies the sender or recipient of a communication or their location;
- identifies or selects the apparatus used to transmit the communication;

- comprises signals which activate the apparatus used (or which is to be used to) to transmit the communication; and
- identifies data as being part of a communication.

2.21 Communications data under this limb also includes data held or capable of being obtained, by the CSP which is logically associated with a communication for the purposes of the telecommunications system by which the communication is being, or may be, transmitted. This might include, for example domain name service (DNS) requests which allow communications to be routed across the network. It also includes data that facilitates the transmission of future communications (regardless of whether those communications are, in fact, transmitted).

2.22 Only information falling within this second limb can be obtained directly from a telecommunications system by a public authority.

2.23 The third limb covers other information held by a CSP about the use of the service such as billing information.

2.24 The fourth limb additionally includes data held by a CSP about the architecture of the telecommunications system (sometimes referred to as 'reference data'). This may include the location of cell masts or Wi-Fi hotspots. This information itself does not contain any information relating to specific persons and its acquisition in its own right does not interfere with the privacy of any customers. However, this data is often necessary for the public authority to interpret the data received in relation to specific communications or users of a service.

2.25 Examples of communications data include, but are not limited to:

- 'subscriber checks' (also known as 'reverse look ups') such as "who is the subscriber of phone number 01632 960 224?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus/devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes[5];
- information about selection of preferential numbers or discount calls;
- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);

[5] This includes PUK (Personal Unlocking Key) codes for mobile phones. These are initially set by the handset manufacturer and are required to be disclosed in circumstances where a locked handset has been lawfully seized as evidence in criminal investigations or proceedings.

- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- itemised telephone call records (numbers called)[6];
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded; and
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

Content

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

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

2.28 When a communication is sent over the telecommunication systems it can be carried by multiple providers. Each provider may need a different set of data in order to route the communication to its eventual destination. Where data attached to a communication is identified as communications data it continues to be communications data, even if certain providers have no reason to look at this data. The definition of content ensures that the elements of a communication which are considered to be content do not change depending on which communication provider is carrying the communication.

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

---

[6] Itemised bills can include an indication of the cost for receiving communications, for example calls and messages received by a mobile telephone that has been ‘roaming’ on another network.

2.30 The second makes clear that systems data cannot be content[7].

Guidance on definitions

2.31 The Home Office may, from time to time, issue further guidance to CSPs or public authorities, on how the definitions in the Act apply.

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

3 General information on bulk acquisition

3.1 Bulk acquisition warrants authorise a two stage process. First, the obtaining of BCD from a CSP and second, the selection for examination of the BCD obtained under the warrant.

3.2 A bulk acquisition warrant will be served on a CSP to require that CSP to disclose the communications data specified in the warrant. This may also require a CSP to obtain and disclose specified communications data that is not in its possession but that it is capable of obtaining.

3.3 A warrant will normally provide for the provision of communications data as it is generated or processed by the CSP for business purposes, but may also relate to the provision in bulk of communications data retained by a CSP for business purposes or under the provisions in Part 4 of the Act. This may result in the collection of large volumes of communications data. This is essential to enable communications relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation.

3.4 In contrast to a targeted communications data authorisation, issued under Part 3 of the Act, a bulk acquisition warrant instrument need not be constrained to a specific operation.

3.5 Chapter 2 of Part 6 does not impose a limit on the volume of communications data which may be acquired. For example, if the requirements of this chapter are met then the acquisition of all communications data generated by a particular CSP could, in principle, be lawfully authorised but only where necessary and proportionate[8] to do so. This reflects the fact that bulk acquisition is an intelligence gathering capability, whereas targeted communications data acquisition is primarily an investigative tool that is used to acquire data in relation to specific investigations.

3.6 Accordingly, and in contrast to targeted communications data acquisition, a warrant may only be sought by a member of the SIA. In addition, the volume of data which may potentially be acquired is reflected in that fact that bulk acquisition warrants must be granted by the Secretary of State and are subject to approval by the Judicial Commissioner. Once acquired in bulk, selection of data for examination is only permitted for approved operational purposes.

3.7 In contrast to the bulk powers provided for in Chapters 1 and 3 of Part 6 of the Act, a bulk acquisition warrant may relate to communications data in relation to individuals in the UK.

[8] See paragraphs 3.8-3.11.

Necessity and proportionality

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

- In the interests of national security, which must always be one of the purposes;
- For the purpose of preventing or detecting serious crime. Serious crime is defined in section 239(1) as crime that comprises an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; or
- In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security. The power to issue a bulk acquisition warrant for the purpose of safeguarding the economic well-being of the UK may only be exercised where it appears to the Secretary of State and Judicial Commissioner that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant for these purposes if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant for the purpose of safeguarding the economic well-being of the UK should therefore identify the circumstances that are relevant to the interests of national security. The power to issue a bulk acquisition warrant for the purpose of safeguarding the economic well-being of the UK may also only be exercised in circumstances where the information it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.

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

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

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

3.11 The following elements of proportionality should therefore be considered:

- Balancing the extent of the proposed interference with privacy against what is sought to be achieved;

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

Trade Unions

3.12 As set out in clause 147, the fact that the information that would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State. The security and intelligence agencies are permitted to apply for a warrant against members or officials of a trade union considered to be a legitimate intelligence target where that is necessary for one of the statutory purposes and proportionate to what is sought to be achieved.

4 Giving of bulk acquisition warrants

Application for a bulk acquisition warrant

4.1 An application for a bulk acquisition warrant is made to the Secretary of State. As set out in section 147 of the Act, bulk acquisition warrants are only available to the intelligence agencies. An application for a bulk acquisition warrant therefore may only be made by or on behalf of the following persons:

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

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

4.3 Prior to submission, each application is subject to a review within the agency making the application. This involves consideration of whether the application is necessary for one or more of the permitted statutory purposes (in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security). One of the statutory purposes for which a bulk acquisition warrant can be issued must always be national security.

4.4 The scrutiny of the application will also include whether the proposed acquisition of communications data in bulk is both necessary and proportionate and whether the examination of that material is, or may be, necessary for one or more of the operational purposes specified.

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

- Description of the BCD to be acquired, details of any CSP(s) and an assessment of the feasibility of the operation where this is relevant and to the extent known at the time of the application[9];
- Description of the conduct to be authorised, which must be restricted to the obtaining of BCD, or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant;
- The operational purposes for which the BCD may be selected for examination;
- An explanation of why the acquisition of BCD is considered to be necessary for one or more of the statutory purposes, which must always include an explanation of why the acquisition of the data is necessary in the interests of national security;

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

- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, explaining why less intrusive alternatives have not been or would not be as effective;
- An assurance that the BCD will be selected for examination only so far as it is necessary for one or more of the operational purposes specified in the warrant and it meets the conditions of section 160 of the Act; and
- An assurance that all BCD will be kept for no longer than necessary and handled in accordance with the safeguards required by section 159 of the Act.

Format of a bulk acquisition warrant

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

- A description of the communications data to be acquired;
- The steps a CSP must take to give effect to the warrant;
- The operational purposes for which any BCD obtained under the warrant may be selected for examination;
- The warrant reference number; and
- Details of the persons who may subsequently modify the operational purposes specified on the warrant in an urgent case.

Authorisation of a bulk acquisition warrant

Necessity

4.7 Before issuing a warrant under Chapter 2 of Part 6 of the Act, the Secretary of State and Judicial Commissioner must consider that the warrant is necessary for one or more of the statutory purposes, as at sections 147(1)(a) and 147(2). If the Secretary of State or Judicial Commissioner is not satisfied that the warrant is necessary in the interests of national security, then it cannot be issued.

4.8 Before issuing a bulk acquisition warrant, the Secretary of State and Judicial Commissioner must also consider that the selection for examination of BCD obtained under the warrant is necessary for one or more of the specified operational purposes (section 147(1)(c)). Setting out the operational purposes on the warrant limits the purposes for which BCD collected under the warrant can be selected for examination. When considering the specified operational purposes, the Secretary of State and Judicial Commissioner must also be satisfied that selection for examination of BCD is necessary for one or more of the statutory purposes set out on the warrant (as at 147(1)(a) and 147(2)). For example, if a bulk acquisition warrant is issued in the interests of national security and for the purpose of preventing or detecting serious crime, every specified operational purpose on that warrant must be necessary for one or both of these two broader purposes.

4.9 The Secretary of State has a duty to ensure that arrangements are in force for securing that only that material which has been considered necessary for examination for a section 147(1)(a) or section 147(2) purpose, and which meets the conditions set out in section 160 is, in fact, selected for examination. The Investigatory Powers Commissioner is under a duty to review the adequacy of those arrangements.

Proportionality

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

4.11 In considering whether a bulk acquisition warrant is necessary and proportionate, the Secretary of State and Judicial Commissioner must take into account whether the information it is considered necessary to obtain under the warrant could reasonably be obtained by other means (section 147(5) of the Act). This consideration should include whether the required information could reasonably be obtained through a less intrusive power such as the targeted acquisition of communications data or the targeted acquisition of communications data using the request filter.

Safeguards

4.12 Before issuing a warrant, the Secretary of State must consider that satisfactory arrangements are in force in relation to the warrant setting out the safeguards for the copying, dissemination, retention and access to BCD. These safeguards are explained at chapters 8 and 9 below.

Judicial Commissioner approval

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

4.14 Section 148 of the Act sets out the factors that a Judicial Commissioner must consider when deciding whether to approve the decision to issue a bulk acquisition warrant. The Commissioner must review the Secretary of State's conclusions as to:

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

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

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

- not issue the warrant; or

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

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

5 Modifications, renewals, and cancellation

Modification of a bulk acquisition warrant

5.1 A bulk acquisition warrant may be modified by an instrument issued by the person permitted to do so under the provisions at section 153 of the Act. A bulk acquisition warrant may be modified to add, vary or remove an operational purpose for which BCD obtained under the warrant may be selected for examination.

5.2 If an agency requires a change in the scope of the data to be obtained under a warrant or a change to the statutory purpose for which the warrant is issued then an additional or replacement warrant must be sought. Nothing in section 153 of the Act permits, by modification, the addition of an operational purpose which is not relevant to the statutory purposes in relation to which the warrant has been issued.

5.3 In circumstances where a modification is being made to add or vary an operational purpose, the modification must be made by a Secretary of State and must be approved by a Judicial Commissioner before the modification comes into force. The considerations set out in chapter 4 apply to a modification as they do to the issuing of a new warrant.

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

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

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

Urgent modifications of a bulk acquisition warrant

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

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

Renewal of a bulk acquisition warrant

5.9 The Secretary of State may renew a warrant within the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect (section 152 of the Act), with the approval of the Judicial Commissioner. Applications for renewalsare made to the Secretary of State and contain an update of the matters outlined in paragraph 4.5 above. In particular, the applicant must give an assessment of the value of the BCD obtained under the warrant to date and explain why it is considered that obtaining the data continues to be necessary in the interests of national security as well as, where applicable, either or both of the purposes in section 147(2), and why it is considered that obtaining of communications data in bulk continues to be proportionate.

5.10 In deciding to renew a bulk acquisition warrant, the Secretary of State must also consider that the selection for examination of BCD obtained under it continues to be necessary for one or more of the specified operational purposes, and that any examination of that material for these purposes is necessary for one or more of the statutory purposes (at 147(1)(a) and 147(2)) on the warrant.

5.11 In the case of a renewal of a bulk acquisition warrant that has been modified so that it no longer authorises or requires the acquisition of BCD, it is not necessary for the Secretary of State to consider that acquisition of BCD continues to be necessary before making a decision to renew the warrant.

5.12 Where the Secretary of State and Judicial Commissioner are satisfied that the warrant continues to meet the requirements of the Act, the Secretary of State may renew it. The renewed warrant is valid for six months from the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed

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

Warrant cancellation

5.14 The Secretary of State, or a senior official acting on their behalf, may cancel a bulk acquisition warrant at any time. Such persons must cancel a bulk acquisition warrant if, at any time before its expiry date, they are satisfied that the warrant is no longer necessary on the purposes of any one of the statutory purposes (at 147(1)(a) and 147(2)) for which it was issued. Such persons must also cancel a warrant if, at any time before its expiry date, he or she is satisfied that the examination of BCD is no longer necessary for any of the operational purposes specified on the warrant. Agencies will therefore need to keep their warrants under continuous review and must notify the Secretary of State if they assess that the warrant is no longer necessary. In practice, the responsibility to cancel a warrant will be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State.

5.15 The cancellation instrument will be addressed to the person to whom the warrant was issued. A copy of the cancellation instrument should be sent to those CSPs who have given effect to the warrant during the preceding twelve months.

5.16 The cancellation of a warrant does not prevent the Secretary of State, with Judicial Commissioner approval, issuing a new warrant, covering the same, or different data and operational purposes, in relation to the same CSP in the future should it be considered necessary and proportionate to do so.

5.17 Where there is a requirement to modify the warrant, other than to vary the operational purposes for which the data can be selected for examination, then the warrant may be cancelled and a new warrant issued in its place.

6 Implementation of warrants and CSP compliance

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

6.2 Section 158 of the Act then allows the agency to carry out the acquisition of BCD, or to require the assistance of other persons in giving effect to the warrant. Section 158 makes clear that the warrant may be served on any person, inside or outside the UK, who is required to provide assistance in relation to that warrant.

6.3 Where a copy of the warrant has been served on a CSP, that person is under a duty to take all such steps for giving effect to the warrant as are notified to him or her by or on behalf of the person to whom the warrant is addressed. This applies to any company offering services to customers in the UK, irrespective of where the company is based.

6.4 The implementing authority must take steps to bring the contents of the warrant to the attention of the relevant person. The Act provides that service of a copy of a warrant on a person outside the UK may (in addition to electronic or other means of service) be effected in any of the following ways:

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

6.5 The duty of compliance is enforceable against a person in the UK by civil proceedings by the Secretary of State for an injunction, or in Scotland for specific performance of a statutory duty under section 45 of the Court of Session Act 1988 or for any other statutory relief.

Provision of reasonable assistance to give effect to a warrant

6.6 Any CSP may be required to provide assistance in giving effect to a bulk acquisition warrant. A warrant can only be served on a person who is capable of providing the assistance required by the warrant. Section 158 places a requirement on CSPs to take all such steps for giving effect to the warrant as are notified to them. The duty to comply with the warrant can only be enforced against a person who is capable of complying with it. Where a technical capability notice is in place, a CSP will be considered to have put in place the capabilities specified in that notice when consideration is given to their compliance with the obligation.

6.7 The steps which may be required are limited to those which it is reasonably practicable to take (section 158(3)). What is reasonably practicable should be agreed after consultation between the CSP and the Government. Such consultation is likely to include consideration of a number of factors including, but not limited to, the technical feasibility and likely cost of complying with any steps notified to the CSP. As part of the consultation, the CSP may raise any other factor that they consider relevant to whether the taking of such steps is reasonably practicable. If no agreement can be reached it will be for the Secretary of State to decide whether to proceed with civil proceedings.

6.8 Where the relevant agency requires the assistance of a CSP in order to implement a warrant, it may provide the following to the CSP:

- A copy of the signed and dated warrant with the omission of the operational purposes and any or all of the other schedules; and/or
- A copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant. Warrants must specify the BCD to be obtained and the operational purposes for which any BCD obtained under the warrant may be selected for examination but CSPs will not receive a copy of the operational purposes specified in the warrant; and/or
- An optional covering document from the relevant agency (or the person acting on behalf of the agency) may also be provided requiring the assistance of the CSP and specifying any other details regarding the means of acquisition of the data and delivery as may be necessary. Contact details with respect to the relevant agency will be made available to the CSP.

Offence of unauthorised disclosure

6.9 A CSP served with a bulk acquisition warrant must keep the warrant secret. The offence of unauthorised disclosure occurs when any CSP, or employee of a CSP, reveals the content or existence of a warrant.

6.10 It is a reasonable excuse for a CSP to disclose the existence or content of a warrant with the permission of the Secretary of State. This is likely to include disclosure:

- To a person (such as a system provider) who is working with the CSP to give effect to the notice; and
- To relevant oversight bodies.

7 Maintenance of a technical capability

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

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

7.3 The obligations the Secretary of State considers reasonable to impose on such persons are set out in regulations made by the Secretary of State and approved by Parliament, and may include (amongst others) the obligations set out in section 229(4) of the Act:

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

7.4 An obligation placed on a CSP to remove encryption only relates to electronic protections that the company has itself applied to the data, or where those protections have been placed on behalf of that CSP. The purpose of this obligation is to ensure that the data can be provided in intelligible form. References to protections applied on behalf of the CSP include circumstances where the CSP has contracted a third party to apply electronic protections to a telecommunications service offered by that CSP to its customers.

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

7.6 While an obligation to remove encryption may only relate to protections applied by or on behalf of the company on whom the obligation is placed, there will also be circumstances where a CSP removes encryption from data for their own business reasons. Where this is the case a public authority will also require the CSP, where applicable and when served with a warrant, to provide that data in an intelligible form.

Consultation with service providers

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

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

Matters to be considered by the Secretary of State

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

7.10 As part of the decision the Secretary of State must take into account, amongst other factors, the matters specified in section 229(3):

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

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

- Whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means
- The public interest in the integrity and security of telecommunications systems and postal services, and
- Any other aspects of the public interst in the protection of privacy.

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

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

Giving a technical capability notice

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

7.15 Section 229(8) provides that obligations may be imposed on, and technical capability notices given to, a CSP located outside the UK and may require things to be done outside the UK. Where a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given to the CSP:

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

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

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

Disclosure of technical capability notices

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

7.19 Any person to whom a technical capability notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence or contents of that notice to any person[10].

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

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

Regular review

7.21 The Secretary of State must keep technical capability notices under review. This helps to ensure that the notice itself, or any of the requirements or restrictions imposed by it, remains necessary and proportionate.

[10] See section 231(8)

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

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

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

- a significant change in demands by agencies that calls into question the necessity and proportionality of the notice as a whole, or any element of the notice;
- a significant change in CSP activities or services; or
- a significant refresh or update of CSP systems.

7.25 The process for reviewing a notice is similar to the process for giving a notice. The Government will consult the communications service provider as part of the review. Once this process is complete, the Secretary of State will consider whether the notice remains necessary and proportionate.

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

Variation of technical capability notices

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

7.28 CSPs subject to a technical capability notice must notify the Government of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require the CSP to provide a technical capability on the new service.

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

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

- a CSP launching new services;
- changing demands and priorities of the security and intelligence agencies
- a recommendation following a review (see section beginning at 7.21); or
- to amend or enhance the security requirements.

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

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

7.33 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraphs 7.9 – 7.13.

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

Revocation of technical capability notices

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

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

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

Referral of technical capability notices

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

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

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

7.41 Both bodies must give the relevant CSP and the Secretary of State the opportunity to provide evidence and make representations to them before reaching their conclusions. Both bodies must report these conclusions to the person who made the referral and the Secretaty of State.

7.42 After considering reports from the TAB and the Commissioner, the Secretary of State may decide to vary, withdraw or confirm the effect of the notice. Where the Secretary of State decides to confirm or vary the notice, the Investigatory Powers Commissioner must approve the decision.Until the Secretary of State's decision is approved, there is no requirement for the communciations service provider to comply with the notice so far as referred. The CSP will remain under obligation to provide assistance in giving effect to a bulk acquisition warrant, as set out in section 157 of the Act.

Contribution of costs for the maintenance of a technical capability

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

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

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

8 General safeguards

8.1 All BCD must be handled in accordance with safeguards which the Secretary of State has approved in line with the duty imposed on him or her by the Act. These safeguards are made available to the Investigatory Powers Commissioner, and they must meet the requirements of section 159 of the Act. Breaches of these safeguards must be reported to the Investigatory Powers Commissioner as agreed with him or her. The agencies must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, the agencies must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

8.2 Section 159 of the Act requires that disclosure, copying and retention of BCD obtained under the warrant is limited to the minimum necessary for the authorised purposes. Section 159(3) of the Act provides that something is necessary for the authorised purposes if the BCD:

- Is, or is likely to become, necessary in the interests of national security or on any other purposes falling within section 147(2) – namely, for the purpose of preventing or detecting serious crime, or for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well-being of the UK[11];
- Is necessary for facilitating the carrying out of the functions under the Act of the Secretary of State or the person to whom the warrant is addressed;
- Is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal;
- Is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of him or her by his or her duty to secure the fairness of the prosecution; or
- Is necessary for the performance of any duty imposed by the Public Records Act.

Personnel security

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

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

Dissemination of BCD

8.4 BCD, and more typically the intelligence derived from it, will need to be disseminated both within and between agencies, as well as to consumers of intelligence, where necessary in order for action to be taken on it. The number of persons to whom a BCD set is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out in section 159(3) of the Act. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency.

8.5 It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: a BCD set must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the a BCD set to carry out those duties. In the same way, only so much of the BCD set may be disclosed as the recipient needs.

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

8.7 Section 159(9) of the Act stipulates that where BCD is disclosed to the authorities of a country or territory outside the UK, the appropriate agency must ensure BCD is only handed over to overseas authorities if the following requirements are met:

- It appears to the UK agency that the requirements corresponding to the requirements in 159(2) and 159(5) (relating to minimising the extent to which BCD is disclosed, copied, distributed and retained) will apply to the extent that the UK agency considers appropriate; and

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

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

Copying

8.9 BCD may only be copied to the extent necessary for the authorised purposes set out in section 159(3) of the Act. This includes any record referring to a bulk acquisition warrant which includes the identities of the persons to or by whom the material was sent. The restrictions are implemented by requiring special treatment of such copies that are made by recording their making, distribution and destruction.

Storage and transfer of data

8.10 BCD, and all copies of it, must be handled and stored securely, so as to minimise the risk of loss or theft. In particular it must be held so as to be inaccessible to persons without the required level of vetting These requirements to store bulk communications data securely apply to all those who are responsible for handling it, including CSPs. The details of what such a requirement will mean in practice for CSPs will be set out in the discussions they have with officials before being asked to give effect to a warrant.

8.11 Individuals should be granted access only where it is required to carry out their function in relation to one of the authorised purposes set out in section 159(3) of the Act.

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

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

Destruction

8.13 BCD, and all copies, must be marked for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes. In this context, this means taking such steps as might be necessary to make access to the data impossible. If BCD is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 159(3) of the Act.

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

9 Safeguards when selecting BCD for examination

9.1 Section 160 of the Act provides specific safeguards relating to the selection for examination of BCD acquired through a bulk acquisition warrant.

9.2 Sections 160(1) and 160(2) make clear that selection for examination may only take place for one or more of the operational purposes that are specified on the warrant, in line with section 150 of the Act. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination, rather than limiting the information which can be examined per se, and no official is permitted to gain access to the data other than as permitted by these purposes. BCD selected for examination for an operational purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained on any relevant ground. Section 150 makes clear that operational purposes must relate to one or more of the statutory purposes specified on the warrant. However, it is not sufficient under the Act for operational purposes simply to use the wording of one of the statutory purposes. The Secretary of State may not approve the addition of an operational purpose to the central list – and therefore to any bulk warrants – unless he or she is satisfied that the operational purpose is specified in a greater level of detail than the relevant statutory purposes. Operational purposes must therefore describe a clear requirement and contain sufficient detail to satisfy the Secretary of State that intercepted content or secondary data may only be selected for examination for specific reasons.

9.3 Section 153 of the Act provides for a bulk acquisition warrant to be modified such that the operational purposes specified on it can be added to or varied. Such a modificiation is categorised as a major modification, and therefore must be made by the Secretary of State and approved by a Judicial Commissioner before the modification may take effect. In such circumstances, the provisions at section 153 also require that the operational purpose must be approved by the Secretary of State for addition to the central list. If the Secretary of State does not approve the addition of the purpose to the list, the modification to the warrant (to add a new operational purpose) may not be made. The Bill therefore creates a strict approval process in circumstances where an intelligence agency identifies a new operational purpose, which they consider needs to be added to a bulk warrant. The Secretary of State must agree that the operational purpose is a purpose for which selection for examination may take place, and that it is described in sufficient detail such that it should be added to the central list. In addition, the Secretary of State must also consider that the addition of that purpose to the relevant bulk warrant is necessary, taking into account the particular circumstances of the case, before making the modification, and the decision to add the operational purpose must also be approved by a Judicial Commissioner.

9.4 In addition to the central list of operational purposes having to be approved by the Secretary of State, section 153 makes clear that it must also be reviewed on an annual basis by the Prime Minister and it must be shared every three months with the Intelligence and Security Committee.

9.5 More than one operational purpose may be specified on a single bulk warrant; this may, where the necessity and proportionality test is satisfied, include all operational purposes currently specified on the central list maintained by the heads of the security and intelligence agencies. In the case of bulk acquisition, BCD relevant to a number of operational purposes may be acquired on a single warrant. In the majority of cases, it will therefore be necessary for bulk acquisition warrants to specify the full list of operational purposes.

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

9.7 In general, automated systems must, where technically possible, be used to effect the selection of BCD in accordance with section 160 of the Act. As an exception, BCD may be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the material falls within the main categories to be selected under the specified operational purposes, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary for the purposes specified in sections 147(1)(a) and 147(2) of the Act.

9.8 Once those functions have been fulfilled, any copies made of the BCD for those purposes must be destroyed in accordance with section 159(5) of the Act. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the Investigatory Powers Commissioner during his or her inspections.

9.9 BCD should be selected for examination only by authorised persons who receive appropriate training regarding the provisions of the Act and specifically the operation of section 160 and the requirements of necessity and proportionality. These requirements and procedures must be set out in internal guidance provided to all authorised persons and the attention of all authorised persons must be specifically directed to the statutory safeguards. All authorised persons must be appropriately vetted.

9.10 Prior to an authorised person accessing the data a record[12] should be created setting out why access to BCD is required consistent with, and pursuant to, section 160 and the applicable operational purpose(s), and why such access is proportionate. Save where the material or automated systems are being checked as described in paragraph 9.9, the record must indicate, by reference to specific factors, the material to which access is being sought and systems should, to the extent possible, prevent access to the material unless such a record has been created. Where it is anticipated that the access to the BCD is likely to give rise to collateral intrusion to privacy, the reasons this is considered proportionate, and any steps to minimise it, must also be recorded. All records must be retained for the purposes of subsequent examination or audit.

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

9.11 Periodic audits should be carried out to ensure that the requirements set out in section 159 of the Act are being met. These audits must include checks to ensure that the records requesting access have been correctly compiled, and specifically, that the material requested falls within operational purposes the Secretary of State has considered necessary for examination. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards must be reported to the Investigatory Powers Commissioner. Where appropriate all intelligence reports generated by the authorised persons must be subject to a quality control audit.

9.12 The Secretary of State must ensure that the safeguards are in force before any acquisition under a bulk acquisition warrant can begin. The Investigatory Powers Commissioner is under a duty to review the adequacy of the safeguards. In particular, in reviewing the adequacy of bulk acquisition safeguards, the Commissioner should give specific consideration to the central list of operational purposes maintained by the heads of the security and intelligence agencies and the use of these purposes on bulk acquisition warrants.

Selection for examination of data relating to those in certain professions

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

9.14 However the degree of interference with an individual's rights and freedoms may be higher where BCD is being selected for examination with the intention of identifying data which relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament[13], or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.

9.15 Such situations do not preclude selecting the data for examination. However investigators, giving special consideration to necessity and proportionality, must take into account any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken when considering whether data should be selected for examination in such circumstances, including additional consideration of whether there might be unintended consequences of such examination and whether the public interest is best served by the data being selected for examination.

[13] References to a Member of Parliament include references to a Member of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

9.16 The nature of bulk data means that in many cases, the officer will not know who the communications data relates to at the point of its selection. However, officers must clearly note in all cases where it is intended or known that the data being selected for examination includes, or is likely to include, communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That fact that such data has been selected for examination must be recorded (see section 10 on keeping of records for more details), including recording the profession, and, at the next inspection, such records should be flagged to the Commissioner.

Selection for examination to determine the source of journalistic information

9.17 Issues surrounding the infringement of the right to freedom of expression may arise if BCD is selected for examination for the purpose of identifying the communications data of an identified or suspected journalist takes place. There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously. Where BCD is selected for examination in order to determine the source of journalistic information, there must therefore be an overriding requirement in the public interest.

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

9.19 An assessment of whether someone is a journalist (for the purposes of the Act) should be made on all the facts and circumstances available at that time. Consideration should be given, in particular, to the frequency of an individual's relevant activities, the level of professional rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest.In the exceptional event that an officer were to select for examination BCD specifically in order to determine a journalist's source, they should only do this if the proposal had been approved beforehand by a person holding the rank of Director or above within their organisation level. Any communications data obtained and retained as a result of such access must be reported to the Investigatory Powers Commissioner at the next inspection.

9.20 Communications data that may be considered to determine journalistic sources includes data relating to:

- journalists' communications addresses;
- the communications addresses of those persons suspected to be a source; and
- communications addresses of persons suspected to be acting as intermediaries between the journalist and the suspected source.

9.21 Where the officer suspects wrong-doing that includes communications with a journalist, the application must consider properly whether that conduct is of a sufficiently serious nature for rights to freedom of expression to be interfered with where communications data is to be selected for examination for the purpose of identifying a journalist's source.

9.22 The requirement for senior approval does not apply where the intent is to examine BCD to identify the communications data of a journalist, but it is not intended to determine the source of journalistic information (for example, where the journalist is suspected of involvement in terrorist activity).

9.23 In such cases there is nevertheless a risk of collateral intrusion into legitimate journalistic sources. In such a case, particular care must therefore be taken to ensure that the officer considers whether the intrusion is justified, giving proper consideration to the public interest. The officer needs to consider whether alternative evidence exists, or whether there are alternative means for obtaining the information being sought.

10 Record keeping and error reporting

Records

10.1 Records must be available for inspection by the Investigatory Powers Commissioner. The oversight regime allows the Investigatory Powers Commissioner to inspect the warrant application upon which the Secretary of State's decision is based, and the agency may be required to justify the content of the warrant.

10.2 Records must also be retained to allow the Investigatory Powers Tribunal, established under the Regulation of Investigatory Powers Act (RIPA), to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of RIPA), particularly where continuing conduct is alleged. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to five years.

10.3 Each agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:

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

10.4 Records should also be kept of the arrangements for securing that BCD has only been accessed for the specified operational purposes. Records should be kept of the arrangements by which the requirements of section 159(2) (minimisation of copying and distribution of bulk communications data), section 159(5) (destruction of bulk communications data) and section 160 (examination of bulk communications data) are to be met.

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

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

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

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

10.7 For each bulk acquisition warrant issued by the Secretary of State and approved by a Judicial Commissioner, the relevant agency must also keep a record of the following:

- The section 147(1)(a) and section 147(2) purpose(s) specified on the warrant;
- The details of modifications made to add, vary or remove an operational purpose from the warrant;
- The number of modifications made to add or vary an operational purpose that were made on an urgent basis;
- The number of modifications made to add or vary an operational purpose (including on an urgent basis) that were refused by a Judicial Commissioner; and
- The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse to modify a bulk acquisition warrant.

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

Errors

10.9 Proper application of the Act and thorough procedures for operating its provisions, including the careful preparation and checking of warrants and authorisations, should reduce the scope for making errors whether by public authorities or by CSPs.

10.10 An error can only occur after a warrant has been issued and the acquisition of data has been initiated.

10.11 Any failure by an agency to apply correctly the process of acquiring, or selecting for examination, BCD set out in this code will increase the likelihood of an error occurring.

10.12 Where any error occurs in the granting of a warrant, or any conduct undertaken to comply with a warrant, a record should be kept.

10.13 Where an error results in BCD being acquired or selected for examination wrongly, a report must be made to the Commissioner. Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, result in the individual being wrongly detained or wrongly accused of a crime as a result of that error. An error as set out in this code constitutes a relevant error for the purposes of section 209 of the Act (see section on serious errors beginning at paragraph 10.22).

10.14 This section of the code cannot provide an exhaustive list of possible causes of errors, however, examples could include:

BCD acquisition

- a warrant is not cancelled when the requirement to acquire the data is known to be no longer valid;
- human error, such as incorrect transposition of information from an application to a warrant where BCD is acquired; or
- over-collection caused by software or hardware issues.

BCD disclosure

- disclosure of the wrong data by a CSP when complying with the warrant; or
- disclosure of communications data by a CSP to the wrong public authority.

BCD access

- there has been material failure to adhere to the safeguards in sections 159 and 160 of the Act;
- communications data obtained under the warrant is selected on a basis that is not necessary and proportionate in all the circumstances; or
- selected communications data is examined on a basis that is not necessary for the fulfilment of one or more of the operational purposes specified in the warrant.

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

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

10.17 All errors should be reported as they arise. If the report relates to an error made by a CSP, the public authority should also inform the CSP and Commissioner of the report in written or electronic form. This will enable the CSP and Commissioner to investigate the cause or causes of the reported error.

10.18 The report sent to the Commissioner by an agency in relation to an error must include details of the error, identified by the agency's unique reference number of the relevant authorisation, explain how the error occurred, indicate whether any unintended collateral intrusion has taken place and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. When an agency reports an error made by a CSP, the report must include details of the error and indicate whether the CSP has been informed or not (in which case the agency must explain why the CSP has not been informed of the report).

10.19 Where a CSP discloses BCD in error, it must report each error to the Commissioner within no more than five working days of the error being discovered. It is appropriate for a person holding a suitably senior position within a CSP to do so, identifying the error by reference to the relevant warrant and providing an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. Errors by service providers could include responding to a warrant by disclosing incorrect data or by disclosing the required data to the wrong agency[14].

10.20 In circumstances where a reportable error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal (see section 12).

10.21 Where material which has no connection to the data authorised for acquisition under the warrant obtained by an agency is disclosed in error by a CSP, that material and any copy of it (including copies contained in or as attachments in electronic mail) should be destroyed as soon as the report to the Commissioner has been made.

[14] This does not affect a CSPs statutory duty under regulation 5A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 to notify the Information Commissioner of a personal data breach. Further guidance is available from the Information Commissioner's website, ico.org.uk

Serious errors

10.22 Section 209 of the Act states that the Commissioner must inform a person of any relevant error relating to that person which the Commissioner consider to be a serious error and that it is in the public interest for the person concerned to be informed of the error.

10.23 In circumstances where an error is deemed to be of a serious nature, the Commissioner may therefore investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

10.24 If the Commissioner concludes that the error is a serious error, the Commissioner must also decide whether it considers that it is in the public interest for the person concerned to be informed of the error. The Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned; and
- the extent to which disclosing the error would be contrary to the public interest or prejudicial to:
  - national security
  - the prevention or detection of serious crime
  - the economic well-being of the United Kingdom; or
  - the continued discharge of the functions of any of the intelligence services.

10.25 Before making its decision, the Commissioner may require the agency which has made the error to make submissions on the matters above.

11 Costs

Making of contributions

11.1 Section 225 of the Act recognises that CSPs incur expenses in complying with warrants under Chapter 2 of Part 6 of the Act. The Act, therefore, allows for appropriate payments to be made to them to cover these costs. The following sections outline the circumstances where the Government will make contributions towards the costs of complying with the Act.

11.2 Significant public funding is made available to CSPs to ensure that they can provide, outside of their normal business practices, an effective and efficient response to warrants. It is legitimate for a CSP to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to facilitate the timely disclosure of the BCD specified in the warrant.

11.3 This is especially relevant for CSPs which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems. Contributions may also be appropriate towards costs incurred by a CSP which needs to update its systems to maintain, or make more efficient, its disclosure process.

11.4 Any CSP seeking to recover appropriate contributions towards its costs should make available to the requesting agency such information as they require, in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the CSP.

11.5 As costs are reimbursed from public funds, CSPs should take into account value for money when procuring, operating and maintaining the infrastructure required to comply with a notice. As changes to business systems may necessitate changes to systems put in place to comply with a warrant, CSPs should take this into account when making any changes to business systems.

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

Costs in relation to a technical capability notice

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

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

11.9 Costs that may be recovered could include those related to the procurement or design of systems required to acquire communications data, their testing, implementation, continued operation and, where appropriate, sanitisation and decommissioning. Certain overheads may be covered if they relate directly to costs incurred by CSPs in complying with their obligations outlined above. This is particularly relevant for CSPs that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems. However, where a CSP expands or changes its network for commercial reasons, it is expected to meet any capital costs that arise.

Power to develop compliance systems

11.10 In certain circumstances it may be more economical for products to be developed centrally rather than CSPs creating multiple different systems to achieve the same end. Where multiple different systems exist it can lead to increased complexity, delays and cost in updating systems (such as for security updates).

11.11 Section 226 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop systems to support the disclosure of BCD. Such systems could operate in respect of multiple powers under the Act.

11.12 Where such systems are developed for use in CSPs the Secretary of State or agency will work closely with CSPs to develop systems which can be properly integrated into their networks. CSPs using such systems will have full sight of any processing of their data carried out by such systems. The Home Office should consult the Commissioner where relevant.

12 Oversight

12.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner, whose remit is to provide oversight of the use of the powers contained within Chapter 2 of part 6 of the Act. By statute the Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others qualified to assist the Commissioner in his or her work.

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

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

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

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

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

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

12.8 The Commissioner must also inform the affected individual of their right to apply to the Investigatory Powers Tribunal (see Complaints section for more information on the Investigatory Powers Tribunal) who will be able to fully investigate the error and decide if a remedy is appropriate.

12.9 Further information about the Investigatory Powers Commissioner, their office and their work may be found at:

13 Contacts / Complaints

General enquiries relating to bulk acquisition

13.1 The Home Office is responsible for policy and legislation regarding bulk acquisition of communications data under chapter 2 of Part 6 of the Act. Any queries should be raised by contacting:

Communications Data Policy Team
Home Office
2 Marsham Street
London
SW1P 4DF

commsdata@homeoffice.x.gsi.gov.uk

Complaints

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

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

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

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

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

This code of practice relates to the powers and duties conferred or imposed under Chapter 2 of Part 6 of the Investigatory Powers Act relating to the acquisition of communications data in bulk by the security and intelligence agencies.

It provides guidance on:

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

This code is aimed at members of the security and intelligence agencies who are involved in the acquisition of communications data in bulk and its storage, handling and selection for examination. It is also aimed at communications service providers' staff involved in the lawful disclosure of communications data under the Act.