Home Office

Communications Data

DRAFT Code of Practice

Autumn 2016

Communications Data

DRAFT Code of Practice

Published for consultation alongside the Investigatory Powers Bill

Autumn 2016

Contents

Section 1

Introduction

1 Introduction

1.1 This code of practice relates to the powers and duties conferred or imposed under Parts 3 and 4 of the Investigatory Powers [Act 2016] ('the Act'). Section 2 of this code provides guidance on the procedures to be followed when acquisition of communications data takes place under the provisions in Part 3 of the Act ('Part 3'). Section 3 of this code provides guidance on the procedures to be followed when communications data is retained under Part 4 of the Act ('Part 4').

1.2 Sections 1, 2 and 4 of this code are relevant to relevant public authorities within the meaning of the Act and to communication service providers ('CSPs')[1]. The relevant public authorities are set out in Schedule 4 of the Act.

1.3 Section 12 of the Act (with Schedule 2) abolishes or amends other information gathering powers in law which provided for access to communications data without appropriate safeguards. Accordingly, relevant public authorities for the purposes of Part 3 should not use other statutory powers to obtain communications data from a postal or telecommunications operator unless:

- That power deals with telecommunications operators,postal operators, or a class of such operators;
- That power can be used in connection with the regulation of telecommunications operators, services or systems; or such postal operators or services;[2]
- That power can be used to acquire communications data relating to postal items crossing the United Kingdom border; or
- That power is authorised by a warrant or order issued by the Secretary of State or a person holding judicial office.

1.4 Such powers should only be used to obtain communications data from a CSP where it is not possible for the public authority to obtain the data under the Act[3].

1.5 Relevant public authorities should also not require, or invite, any postal or telecommunications operator to disclose communications data by relying on any exemption to the principle of non-disclosure of personal data set out under Part 4 of the Data Protection Act 1998 ('the DPA').

1.6 Sections 1, 3 and 4 of this code are relevant to CSPs who have been issued with a data retention notice under Part 4.

---

1 See paragraph 2.1 for a definition of communications service provider.

2 The Office of Communications or a statutory co-regulator it approves may, for example, use powers conferred by or under Part 2 of the Communications Act 2003 to obtain communications data from a telecommunications operator for the purpose of carrying out the regulatory functions given to them under that Part of that Act.

3 Section 12(3) provides that regulatory powers and powers which can acquire postal data in relation to items crossing the border may only be exercised by the public authority if it is not possible for the public authority to use a power under the Act to secure the disclosure of the data.

1.7 This code should be readily available to members of a relevant public authority involved in the acquisition of communications data under the Act, and to CSPs involved in the retention of communications data and/or its disclosure to public authorities under the Act.

1.8 The Act provides that persons exercising any functions to which this code relates must have regard to the code. Although failure to comply with the code does not, of itself, make a person liable to criminal or civil proceedings.

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

1.10 The Interception of Communications Code of Practice, Bulk Acquisition Code of Practice and Equipment Interference Code of Practice provide guidance on procedures to be followed in relation to those Parts of the Act.

1.11 The exercise of powers and duties under Parts 3 and 4 of the Act and this code are kept under review by the Investigatory Powers Commissioner ('the Commissioner') appointed under section 205 of the Act and by his Judicial Commissioners and inspectors who work from the Investigatory Powers Commission. Duties under Part 4 of the Act and this code in relation to the security, integrity and destruction of data retained under a notice are subject to audit by the Information Commissioner. CSPs must comply with reasonable requests from the Information Commissioner in relation to his audit role.

1.12 The Home Office may issue further advice directly to public authorities and CSPs as necessary.

1.13 This code extends to the United Kingdom[4].

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

[4] This code and the provisions in Parts 3 and 4 of the Act do not extend to the Crown Dependencies and British Overseas Territories. Note that chapter 11 includes sections on acquisition of communication data on behalf of overseas authorities and the transfer of communications data to overseas authorities.

2 Scope and definitions

Communications service provider

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

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

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

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

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

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

2.7 In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider, or where there are security implications in doing so, the data may be sought from the CSP which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of communications data for example, where a hotel is in possession of data identifying specific telephone calls originating238 of the Act defines 'postal service' to mean any service which consists in one or more of the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items and which is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to transmit postal items from place to place.

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

Composition of communications

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

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

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

Communications data

2.12 The term 'communications data' includes the 'who', 'when', 'where', and 'how' of a communication but not the content i.e. what was said or written[5].

2.13 It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning[6], of the communication.

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

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

Telecommunications definitions

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

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

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

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

---

5 See paragraph 2.45 for the definition of content.

6 As set out at section 237(6)(a)

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

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

- Identifies the sender or recipient of a communication or their location;
- Identifies or selects the apparatus used to transmit the communication;
- Comprises signals which activate the apparatus used (or which is to be used to) to transmit the communication; and
- Identifies data as being part of a communication.

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

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

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

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

2.25 All communications data held by a telecommunication operator or obtainable from a telecommunications system falls into two categories:

- Entity data – This data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).
- Events data – Events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

2.26 The authorisation levels required to access communications data reflect the fact that the set of events data as a whole contains the more intrusive communications data, including information on who has been in communication with whom, a person's location when their mobile device connects to the network and internet connection records. The authorisation levels in Schedule 4 to the Act reflect the differing levels of intrusiveness of the data. For example the police can authorise access to entity data at Inspector level but events data is authorised at Superintendent level.

2.27 There are some circumstances where a CSP will need to process events data in order to respond to a request for entity data. In such circumstances it is the type of data that is disclosed which determines the authorisation level required e.g. if a public authority wants to know the identity of a person using an IP address at a specific time and date then the CSP can provide this response as entity data even though it may have to obtain this information from event data relating to a specific communication.

2.28 Where a public authority provides events data to a CSP as part of a request for entity data then the CSP may include that events data in the response to the entity data request. Taking the example above the CSP could include the time and date of the communication as part of the response without the need for it to be authorised as an event.

Entity data

2.29 Entity data covers information about a person or thing, and about links between a telecommunications service, part of a telecommunication system and a person or thing, that identify or describe the person or thing. This means that individual communication devices such as phones, tablets and computers are entities. The links between a person and their phone are therefore entity data but the fact of or information about communications between devices on a network at a specific time and for a specified duration would be events data.

2.30 Examples of entity data include:

- 'Subscriber checks' such as "who is the subscriber of phone number 01632 960 224?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- Subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- Information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- Information about apparatus/ devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes[7]; and

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

- Information about selection of preferential numbers or discount calls.

2.31 Entity data can change over time. So, for example if a person moves house the address held by a CSP will change. The fact of that is an attribute of the entity (the person) and not a communication event.

2.32 Some CSPs may retain user passwords[8] where already available in the clear for business purposes. In this context passwords would constitute entity data. Any information, such as a password, giving access to the content of any stored communications or access to the use of a communication service may only be sought from a CSP in the following circumstances:

- Where such information is necessary in the interests of national security; or
- For preventing death, injury or damage to health.

2.33 Passwords cannot be used by a public authority to access the content of stored communications or any communication service without appropriate lawful authority, for example the consent of the person, an equipment interference warrant, an interception warrant, property interference authorisation or directed surveillance authorisation.

Events

2.34 Events data covers information about events taking place across a telecommunications system at a specific time and for a specified duration. Communications data is limited to communication events describing the transmission of information between two or more entities over a telecommunication service. This will include information which identifies, or appears to identify, any person, apparatus[9] or location to or from which a communication is transmitted. It does not include non-communication events such as a change in address or telephone number for a customer.

2.35 Examples of events data include, but are not limited to:

- Information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- Information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- Information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- Routing information identifying apparatus through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);

---

[8] In many cases a CSP will actually retain a password hash rather than the password itself. This is an encrypted form of the password. When you enter the password to use a service it is encrypted using the same method and the password hash generated is checked against the hash held by a CSP meaning the CSP never needs to retain the actual passwords. A hash is unlikely to be of any use to a public authority and where that is the case it is unlikely to be sought.

[9] 'Apparatus' is defined in section 239 of the Act to mean 'any equipment, machinery, device (whether physical or logical) and any wire or cable'.

- Itemised telephone call records (numbers called)[10];
- Itemised records of connections to internet services;
- Itemised timing and duration of service usage (calls and/or connections);
- Information about amounts of data downloaded and/or uploaded;
- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

Postal definitions

2.36 Communications data in relation to a postal service is defined at section 238(3) of the Act and includes:

- Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted;
- Data relating to the use made by a person of a postal service;
- Information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service **and** which relates to the provision of the service.

2.37 The data in the first limb includes any information that identifies, or appears to identify, any person or location to or from which a communication is or may be transmitted and includes:

- Anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item's postal routing, sender or recipient;
- Records of correspondence checks comprising details of data from postal items in transmission to a specific address; and
- Online tracking of communications (including postal items and parcels).

2.38 The second limb includes data relating to the use made by any person of a postal service, or any part of it includes:

- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including redirection services;
- The price paid to send an item and the postage class used;
- Records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

2.39 The third limb of the definition includes information about any person to whom a service is provided, whether a subscriber or guest user and whether or not they have ever then used that service. For example this may include information about the person associated with a PO Box even if that PO Box address has never received any mail.

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

2.40 As with the telecommunications definitions this limb does not include data which may be held about a customer by a CSP more generally which are not related to the provision of a postal service.

2.41 Examples of data within the third limb include:

- Information about the subscriber to a PO Box number or a postage paid impression used on bulk mailings;
- Information about the provision to a subscriber or account holder of forwarding/redirection services, including delivery and forwarding addresses;
- Subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments.

2.42 Postal data is defined in section 238(4) of the Act and includes specified categories of data written on the outside of a postal item. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is postal data.

2.43 Those public authorities which are able to authorise access to entity data at a lower level of seniority may also authorise access to the third limb of postal communications data at 238(3)(c) of the Act at the same level.

Content

Telecommunications definitions

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

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

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

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

2.48 The second makes clear that systems data cannot be content[11].

Postal definitions

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

Web browsing and communications data

2.50 Browser software provides one way for users to access web content (although there are other commonly used mechanisms, such as dedicated applications). When using a browser to access the web, a user may enter a web address. These are also referred to as URLs (uniform resource locators).

2.51 The URL is normally converted from a human understandable form to numeric IP addresses by means of DNS in order to transmit information over the internet.

2.52 URLs follow a standardised structure and will always contain:

- The scheme - web data is commonly transferred by the http protocol.
- The host identifier, which can be a fully or partially qualified domain name. A web communication requires the fully qualified domain name (FQDN) in order for the process to be completed. Use of a partially qualified domain name (PQDN) will either end up with a FQDN being generated for the browser, or a failed communication. Some web sites split their content across a number of servers which may be identified by FQDNs, for example news.newssite.co.uk or bbc.co.uk. Because the content is split across a number of servers the fully qualified domain name routes the communication to the correct server.

2.53 These elements of a URL are necessary to route a communication to the intended recipient and are therefore communications data. Although fully qualified domain names provide an indication of the type of content that the server being accessed contains they do not identify individual items of content and therefore the exception to the definition regarding inferred meaning ensures that such elements of the URL are not considered content.

2.54 Additionally URLs may, but do not always, contain:

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

- The port, which is an extended part of the IP address, and is required to make the communication process function.
- The userinfo, which does not have to appear. It covers usernames and authorisations.
- The path and optional parameters, which are analogous to a file path on a computer. In the example of socialmedia.com/profile/home the /profile/home is the path.
- The optional query parameters and fragments. These query parameters (identified by a '?' in the URL) contain data that doesn't fit within a hierarchical path structure and can locate certain content.

2.55 With the exception of the port, and in certain circumstances the userinfo, these elements of a URL, where present, will not constitute communications data.

2.56 An authorisation under Part 3 of the Act or retention notice under Part 4 of the Act may only authorise the acquisition or retention of those elements of a URL which constitute communications data.

Relevant communications data

2.57 A data retention notice under the Act may only require the retention of relevant communications data. Relevant communications data is defined in section 84 of the Act and is a subset of communications data.

2.58 It is data which may be used to identify or assist in identifying any of the following:

- The sender or recipient of a communication (whether or not a person) – this can include phone numbers, email addresses, user identities and other information which can identify a customer such as names, addresses, account details and other contact information. In the context of internet access this can include source and destination IP addresses, port numbers and the relevant elements of URLs[12];
- The time or duration of a communication – this can include the time and duration of phone calls, the time of emails, connections on the internet or internet access sessions;
- The type, method or pattern, or fact, of communication – this can include billing records or other records showing the usage of a communication system;
- The telecommunications system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted – this can include the identities of cell masts or Wi-Fi access points to which a device has connected; or
- The location of any such system – this can include the physical location of phones or other communication devices or the location of cell masts or Wi-Fi access points to which they connect. The data that can be retained under a notice includes the data which would form an internet connection record (see below).

[12] See section on web browsing and communications data, paragraphs 2.50-2.56.

2.59 The data to be retained under a retention notice will be set out in the notice. A notice may provide for the retention of data that is necessary to enable the CSP to correlate the above data and transmit it in response to requests. This may include, but is not limited to, customer reference numbers.

2.60 A data retention notice can never require a CSP to retain the content of communications or third party data (see paragraph 2.68).

Internet connection record

2.61 An Internet connection record ('ICR') is a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet. An ICR is communications data which may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunications system for the purpose of obtaining access to, or running, a computer file or program. It comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication. In most cases ICRs will be held by internet access providers which are telecommunications operators which provide access to the internet and can include a home broadband connection, mobile internet or publicly available Wi-Fi.

2.62 An ICR will only identify the service that a customer has been using. It is not intended to show what a customer has been doing on that service. For example many social media apps on a device maintain persistent connections to a service. Even in this case the relevant ICR will signpost the service accessed by the device, enabling the public authority to make further enquiries of the service provider identified through an ICR. An ICR may consist of:

- A customer account reference – this may be an account number or an identifier of the customer's device or internet connection;
- The date/time of the start and end of the event or its duration;
- The source IP address and port;
- The destination IP address and port – this is the address of the service accessed on the internet and could be considered as equivalent to a dialled telephone number. The port additionally provides an indication of the type of service (for example website, email server, file sharing service, etc.);
- The volume of data transferred in either, or both, directions;
- The name of the internet service or server connected to; and
- Those elements of a URL which constitute communications data – this is the web address which is the text you type in the address bar in an internet browser. In most cases this will simply be the domain name – e.g. socialmedia.com.

2.63 The core information that is likely to be included is: an account reference, a source IP and port address, a destination IP and port address and a time/date. However,

there is no single set of data that constitutes an internet connection record, it will depend on the service and service provider concerned.

2.64 Where a data retention notice is issued requiring a CSP to retain ICR the specific data that an internet access provider may be required to retain will be discussed with the provider before the requirement is imposed[13].

2.65 A CSP cannot be required to retain third party data as part of an ICR.

2.66 ICRs can include connections which are made automatically by a person's browser or device.

Third party data

2.67 Where a communication is sent there may be multiple providers involved in the delivery of the communication. Each provider may require different elements of communications data to route the communication. For example, when sending an email there will be the email provider, the internet access provider for the sender and the internet access provider for the recipient. The email provider will require the email address to route the communication but neither internet access provider has any need to see or access the full email address in order to connect the sender or recipient to the mail server.

2.68 Where one CSP is able to see the communications data in relation to applications or services running over their network, in the clear, but does not process that communications data in any way to route the communication across the network this is regarded as third party data. A CSP is considered to process data to route a communication if it specifically looks at an item of data in order to determine what action to take or if it has a set of rules in place which determine how a communication should be routed depending on certain items of data.

2.69 If a CSP has no need to process data to route a communication but extracts and retains this data or a product generated from this data for their own business purposes, such as for network diagnostics, then this is no longer regarded as third party data. This data could be covered by a data retention notice and is available to be acquired under Part 3 of the Act.

2.70 A retention notice **cannot** require a CSP to retain third party data. Accordingly an ICR retained by a CSP may only include data that the CSP itself needs to transmit the communication, unless the CSP retains additional relevant data about the third party service for their own business purposes.

2.71 A communications data authorisation can permit the acquisition by a public authority of third party data on a forward looking basis where necessary and proportionate in relation to a specific investigation. A CSP in receipt of a request or requirement to obtain and disclose third party data need only provide the data where reasonably practicable to do so. A CSP in receipt of a requirement to obtain and disclose third party data which is encrypted by the third party is under no obligation to decrypt such information.

[13] See paragraph 4.67 on issuing notices.

Guidance on definitions

2.72 Where an applicant is unsure of the category of data they are seeking (entity or events data) or what additional communications data may be retained by a CSP for their own business use, the applicant should discuss this with their Single Point of Contact (SPoC). If a SPoC or designated senior officer wish to find out more, they should consult the relevant CSP or contact the Communications Data Knowledge and Engagement Team, currently part of the College of Policing.

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

Part 2

Communications Data Acquisition and Disclosure

3 General extent of powers

Scope of powers, necessity and proportionality

3.1 The acquisition of communications data under Part 3 of the Act will be a justifiable interference with an individual's human rights under Articles 8 and, in certain circumstances, 10 of the European Convention on Human Rights only if the conduct being authorised or required to take place is necessary for the purposes of a specific investigation or operation, proportionate and in accordance with law.

3.2 The Act stipulates that conduct to be authorised or required must be necessary for one or more of the purposes set out in section 58(7) of the Act:

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder; or
- In the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- In the interests of public safety - this purpose should be used by public authorities with functions to investigate specific and often specialised offences or conduct such as accident investigation or for example, a large scale event that may cause injury to members of the public. Public safety should not be interpreted as for purposes relating to crime that impacts on the public, such as the sale of illegal drugs;
- For the purpose of protecting public health – this should be used by public authorities with functions to investigate specific and often specialised offences or conduct such as breaches of health and safety legislation and criminal offences which may risk public health, for example, the supply of controlled medicines without licence or prescriptions;
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- For the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health – this can include those situations where, for example, there is serious concern for the welfare of a vulnerable person including children at imminent risk of being abused or otherwise harmed. It may also include circumstances where a person is missing and the acquiring authority considers there to be a real threat to that person's life or health;
- To assist investigations into alleged miscarriages of justice;
- Where a person ("P") has died or is unable to identify themselves because of a physical or mental condition to assist in identifying P, or to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition; and
- For the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.

3.3 The purposes for which public authorities may seek to acquire communications data are set out in Schedule 4 to the Act (and for local authorities in section 70). The designated senior officer may only consider necessity on grounds open to their public authority and only in relation to matters that are the statutory or administrative function of their respective public authority. The purposes noted above should only be used by a public authority in relation to the specific (and often specialist) offences or conduct that it has been given the statutory function to investigate.

3.4 As set out in section 58(8), the fact that the information that would be obtained under an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the authorisation is necessary on the grounds on which authorisations may be issued. Public authorities are permitted to apply for an authorisation against members or officials of a trade union where that is necessary for one of the stautory purposes listed above and proportionate to what is sought to be achieved.

3.5 There are further restrictions upon the acquisition of ICRs (see chapter 7). ICRs cannot be acquired by local authorities in any circumstances.

3.6 When a public authority wishes to acquire communications data, the designated senior officer must believe that the acquisition, in the form of an authorisation, is necessary. He or she must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

3.7 As well as consideration of the rights of the individual under investigation, consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. An application for the acquisition of communications data should draw attention to any circumstances which give rise to significant collateral intrusion. In such cases it may be appropriate to utilise the filtering arrangements (see chapter 9).

3.8 Particular consideration must also be given, when pertinent, to the right to freedom of expression and the need to protect the public interest in the confidentiality of sources of journalistic information through judicial approval of relevant applications[14].

3.9 Taking all these considerations into account in a particular case, an interference with the rights of an individual may still not be justified because the adverse impact on the rights of another individual or group of individuals is too severe.

3.10 Any conduct where the interference is excessive in relation to the aims of the investigation or operation, or is in any way arbitrary, will not be proportionate.

[14] See section on applications to determine the source of journalistic information beginning at paragraph 6.5 for further information and guidance.

3.11 Before public authorities can acquire communications data, authorisation must be given by the designated senior officer in the relevant authority. A designated senior officer is someone holding a prescribed office, rank or position (or a more senior position), specified in relation to the relevant authority that has been designated for the purpose of acquiring communications data by section 67 of or Schedule 4 to the Act .

3.12 Section 2 of the Act requires a public authority to have regard to the following when granting an authorisation to obtain communications data:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means,
- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.

3.13 The relevant public authorities are set out in Schedule 4 to the Act.

Further guidance on necessity and proportionality

3.14 Training regarding necessity and proportionality should be made available to all those who participate in the acquisition and disclosure of communications data.

Necessity

3.15 In order to justify that an application is necessary, the application needs as a minimum to cover three main points:

- The event under investigation, such as a crime or vulnerable missing person;
- The person, whose data is sought, such as a suspect, witness or missing person, and how they are linked to the event; and
- The communications data, such as a telephone number or IP address, and how this data is related to the person and the event.

3.16 Necessity should be a short explanation of the event, the person and the communications data and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

Proportionality

3.17 Applications should include an outline of how obtaining the data will benefit the investigation or operation. The relevance of the data being sought should be explained and any considerations which might undermine the application.

3.18 This should include explaining how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example the subscriber details of a phone number may be obtainable from a phone book or other publically available sources.

3.19 The relevance of time periods requested must be explained, outlining how these periods are proportionate to the event under investigation.

3.20 An examination of the proportionality of the application should particularly include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

3.21 Collateral intrusion is the obtaining of any information relating to individuals other than the subject(s) of the investigation. The degree of collateral intrusion forms part of the proportionality considerations, and becomes increasingly relevant when applying for events data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion. When there are no meaningful collateral intrusion risks, such as when applying for entity data in relation to a person under investigation, the absence of collateral intrusion should be noted.

3.22 An examination of the proportionality of the application should also involve a consideration of possible unintended consequences and, when relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application.

3.23 Unintended consequences are more likely in more complicated requests for events data or in applications for the data of those in professions with duties of confidentiality. For example, if a journalist is a victim of crime, applications for events data related to that journalist's phone number as part of the criminal investigation may also return some phone numbers of that journalist's sources, with unintended impact on freedom of expression. Such an application may still be necessary and proportionate but the risk of unintended consequences should be considered. The special considerations that arise in such cases are discussed further in the sections on "Communications data involving certain professions" and "Applications to determine the source of journalistic information".

4 General rules on the granting of authorisations

4.1 Acquisition of communications data under the Act involves four roles within a relevant public authority:

- The applicant;
- The designated senior officer;
- The single point of contact; and
- The senior responsible officer.

4.2 The Act provides for acquisition of communications data, by way of an authorisation under section 58. An authorisation granted to a member of a public authority permits that person to engage in conduct which is for the purpose of obtaining data from any person and relates to a telecommunication system or postal service, or data derived from such a system or service. Such conduct may include requiring by notice a postal or telecommunications operator to disclose the relevant communications data held by it, or to obtain and disclose the data whether or not in existence at the time of the authorisation, when it is reasonably practicable for them to do so, in accordance with the authorisation. Authorisations are explained in more detail within this chapter.

4.3 All authorisations and notices must be granted or cancelled in writing or, if not, in a manner that produces a record within the public authority of it having been granted.

4.4 An authorisation may relate to conduct outside the UK and persons outside the UK. Anyone providing a public postal service or a telecommunications service, or who has control of a telecommunication system in the UK, is under a duty to comply with any requirements imposed by notice given to them in pursuance of an authorisation. This applies to any company offering services to customers in the UK, irrespective of where the company is based.

4.5 An authorisation under section 58 of the Act may not be used to acquire communications data directly from a telecommunications network where equipment is interfered with in the process of acquiring communications data. Such activity includes interference with a user device or the network over which the communication is being carried. Such practices may only take place under an equipment interference warrant – see the equipment interference code of practice.

4.6 An authorisation under section 58 of the Act may not be used where it is not possible to determine whether the data being acquired would constitute communications data. Where there is doubt as to whether data other than communications data would be acquired an interception warrant, or where appropriate equipment interference warrant, should be sought.

The applicant

4.7 The applicant is a person involved in conducting an investigation or operation for a relevant public authority who makes an application in writing or electronically for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the designated senior officer, the necessity and proportionality of a specific requirement for acquiring communications data.

4.8 An application may be made orally in exceptional circumstances, but a record of that application must be made in writing or electronically as soon as possible, and certainly within one working day (paragraphs 4.77 - 4.83 provide more detail on urgent procedures).

4.9 An application[15] must:

- Include the name (or designation where relevant for applicants in the Security and Intelligence Agencies (SIA)) and the office, rank or position held by the person making the application;
- Include a unique reference number;
- Include the operation name (if applicable) to which the application relates;
- Specify the purpose for which the data is required, by reference to a statutory purpose under section 58(7) of the Act;
- Describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- Describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- Explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it[16];
- Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- Consider and, where appropriate, describe any possible unintended consequences of the application;
- Where data is being sought from a CSP, specify whether the CSP may inform the subject(s) of the fact that an application has been made for their data; and
- Identify and explain the time scale within which the data is required.

4.10 The application should record subsequently whether it was approved by a designated senior officer, by whom and when that decision was made. If approved, the application form should, to the extent necessary, be cross-referenced to any authorisation granted. The original or a copy of the application must be retained by the SPoC.

---

[15] Public authorities should ensure their application processes are efficient and do not impose unnecessary bureaucracy on their operational staff which goes beyond the requirements of the Act and this code.

[16] See sub-section on further guidance on necessity and proportionality, beginning at paragraph 3.14. This also applies to the next two bullets on collateral intrusion and unintended consequences.

The designated senior officer

4.11 The designated senior officer is a person holding a prescribed office in a relevant public authority[17]. If the designated senior officer believes the acquisition of communications data is necessary and proportionate in the specific circumstances, an authorisation is granted. If the designated person does not consider the case for obtaining the data has been met the application should be rejected and referred back to the SPoC and the applicant.

4.12 It is the designated senior officer's responsibility to consider the application and record their considerations at the time (or as soon as is reasonably practicable) in writing or electronically. They must be able to show that they have understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny. Comments should be tailored to a specific application as this best demonstrates the application has been properly considered.

4.13 If the designated senior officer having read the application considers the applicant has met all the requirements then he or she should simply record that fact. In such cases a simple note should be recorded. There may be circumstances where the designated senior officer having read the case set out by the applicant and the considerations of the SPoC will want to comment why it is still necessary and proportionate to obtain the data despite excessive data being acquired.

4.14 Individuals who undertake the role of designated senior officer must have current working knowledge of human rights principles and legislation, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data under Part 3 of the Act and this code.

4.15 The existence of a defined cadre of designated senior officers within any given organisation will assist the senior responsible officer and SPoC in managing training and compliance requirements. A 'defined cadre' ensures that authorisation may not be given by anyone at the correct grade but by a listed subset of people or roles at that grade who have the appropriate expertise.

4.16 When considering proportionality, the designated senior officer should apply particular consideration to unintended consequences. The seniority, experience and training of the designated senior officer provides them with a particular opportunity to consider possible unintended consequences. Specific additional proportionality issues relating to use of filtering arrangements are detailed at paragraph 9.8.

4.17 Designated senior officers must ensure that they grant authorisations only for purposes and only in respect of types of communications data that a designated senior officer of their office, rank or position in the relevant public authority may grant or give.

[17] See section 61 and Schedule 4 to the Act.

4.18 Where an investigation relates to an allegation of criminal conduct by a member of a public authority, that public authority (or another public authority appointed to investigate the complaint) may use their powers under Part 3 to obtain communications data for the purpose of preventing or detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain communications data under the Act.

4.19 The designated senior officer shall assess the necessity of any conduct to acquire or obtain communications data taking account of any advice provided by the SPoC.

4.20 Designated senior officers must ordinarily be independent from operations and investigations when granting authorisations related to those operations. In practice this means that a designated senior officer should be far enough removed from the applicant's line management chain or the investigation so as to not be influenced by operational imperatives, such as pressure to expedite results on a particular operation. Normally this will mean that the designated senior officer is not within the same department or unit or an integral part of the investigation. It is not considered good practice for applicants to be able to choose a designated senior officer on a case-by-case basis.

4.21 In exceptional circumstances a public authority may not be able to call upon the services of a designated senior officer who is independent from the investigation or operation. This may include cases where delays in locating an independent designated senior officer may pose an immediate threat to life. Such cases would normally be expected to invoke the urgent oral process.

4.22 Three further exceptions to this rule exist. In these cases the senior responsible officer must inform the Commissioner, in advance, of those designated senior officers who would not be independent in such cases. These exceptions are:

- Specialist criminal investigation departments within public authorities which are not law enforcement or intelligence agencies whose small size precludes use of an independent designated senior officer[18];
- Where the investigation or operation concerned is one where there is an exceptional need, in the interests of national security, to keep knowledge of it to a minimum: and
- Where there is an opportunity to obtain information where the opportunity is rare, the time to act is short, and the need to obtain the information is significant and in the interests of national security.

[18] Small public authorities should consider entering into a collaboration agreement under section 75 of the Act.

4.23 In all circumstances where public authorities use designated senior officers who are not independent from an operation or investigation, the senior responsible officer must notify the Commissioner of circumstances and reasons (noting which designated senior officer granted the authorisation) at the next inspection or as otherwise required by the Commissioner. The details of the public authorities and the reasons such measures are being undertaken may be published and included in the Commissioner's report.

4.24 Where a designated senior officer is not independent from the investigation or operation their involvement and their justification for undertaking the role of the designated senior officer must be explicit in their recorded considerations.

4.25 Particular care must be taken by designated senior officers when considering any application to obtain communications data to identify apparatus (such as a mobile telephone) at or within a location or locations and at or between times on a given date or dates where the identity of the apparatus is unknown[19]. Unless the application is based on information that the apparatus was used or was likely to have been used in a particular location or locations at a particular time or times it will, in practice, be rare that any conduct to obtain communications data will be proportionate or the collateral intrusion justified.

4.26 In situations where there is an immediate threat to life (for example a person threatening to take their own or someone else's life or where threats are made to a victim in a kidnap) some CSPs will undertake to adapt their systems beyond the requirements of their normal business practice to be able to assist the relevant public authority in preserving life. The use of such bespoke systems must be proportionate, and any collateral intrusion justified, to the specific circumstances of any investigation or operation.

4.27 Where there is no immediate threat to life in an investigation or operation, any conduct to obtain communications data using any other bespoke systems (for example, those used to trace malicious and nuisance communications) must be reliant upon both the co-operation and technical capability of the CSP to provide such assistance outside of its normal business practice.

The single point of contact

4.28 Before granting an authorisation a designated senior officer must, except in exceptional circumstances (see paragraphs 4.42 – 4.47), have the benefit of the advice of a SPoC as detailed in section 73 of the Act. This might include situations where the designated senior officer has spoken to the SPoC directly or reviewed advice from the SPoC which is included with the application.

4.29 Public authorities unable to call upon the services of an accredited SPoC should not seek to undertake the acquisition of communications data.

[19] Communications Data Strategy Group is able to offer additional advice to SPoCs where investigations or operations in their public authority are considering the acquisition of such data.

4.30 In circumstances where a CSP is approached by a person who cannot be authenticated as an accredited individual and who seeks to obtain data under the provisions of the Act, the CSP may refuse to comply with any apparent requirement for disclosure of data until confirmation of both the person's accreditation and their duties as a SPoC is obtained from the Home Office.

4.31 Public authorities are expected to provide SPoC coverage for all communications data acquisitions that they reasonably expect to make. Police forces, for example, would expect to deal with threat to life situations at any time and should ensure that a SPoC is always available in such circumstances.

4.32 The SPoC is an accredited individual trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC authentication identifier[20]. Details of all accredited individuals are available to CSPs for authentication purposes.

4.33 An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. This encourages the public authority to regulate itself. The SPoC provides objective judgement and advice to both the applicant and the designated senior officer. In this way the SPoC provides a 'guardian and gatekeeper' function ensuring that public authorities act in an informed and lawful manner.

4.34 Where a number of providers are involved in the provision of a communication service, consultation with the public authority's SPoC will determine the most appropriate plan for acquiring data though it is the designated senior officer who ultimately decides which of the CSPs should be given a notice. With the proliferation of modern communications media, including mobile telephony, internet communications, and social networks, and given that one individual can use many different forms of communications, the knowledge and experience of the SPoC in providing advice and guidance to the designated senor officer is significant in ensuring appropriateness of any action taken to acquire the data necessary for an investigation.

4.35 The SPoC[21] will, as appropriate:

- Assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data[22];
- Advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;
- Engage with applicants to develop and implement effective strategies to obtain communications data in support of operations or investigations;

---

[20] At the time of writing, the authentication identifier is a SPoC Personal Identification Number ('SPoC PIN').

[21] Advice and consideration given by the SPoC in respect of any application may be recorded in the same document as the application and/or authorisation.

[22] In the event that the required data is inextricably linked to, or inseparable from, other events data, the designated senior officer must take that into account in their consideration of necessity, proportionality, collateral intrusion and unintended consequences.

- Advise on and manage the use of filtering arrangements, specifically in relation to progress of requests through the filter and compliance by the filter with the relevant authorisation;
- Advise applicants and designated senior officers on the interpretation of the Act, particularly whether an authorisation is appropriate;
- Provide assurance to designated senior officers that authorisations are lawful under the Act and free from errors;
- Consider and, where appropriate, provide advice to the designated senior officer on possible unintended consequences of the application;
- Provide assurance to CSPs that authorisations and notices are authentic and lawful;
- Assess whether communications data disclosed by a CSP in response to a notice fulfils the requirement;
- Assess whether communications data obtained by means of an authorisation fulfils the requirement of the authorisation;
- Assess any cost and resource implications to both the public authority and the CSP of data requirements; and
- Provide advice to the applicant and designated senior officer on when it may be appropriate to require use of the request filter in fulfilling an authorisation (see chapter 9 for more detail).

4.36 The SPoC would normally be the person who takes receipt of any communications data acquired from a CSP and would normally be responsible for its dissemination to the applicant. SPoCs in public authorities should be security cleared in accordance with their own organisation's requirements. When handling, processing, and distributing such information, SPoCs must comply with local security policies and operating procedures. Communications data acquired by public authorities must also by stored and handled in accordance with duties under the Data Protection Act[23].

4.37 Despite the name, in practice many organisations will have multiple SPoCs, working together. Nonetheless, in the course of a joint investigation between authority A with no SPoC and authority B with a SPOC and communications data acquisition powers, authority B may, where necessary and proportionate, acquire communications data under the Act to further the joint investigation.

4.38 For each individual application, the roles of SPoC and designated senior officers or SPoC and applicant will normally be carried out by two persons, depending on how a public authority uses its SPoCs. In exceptional cases, such as those covered under the urgent oral procedure or, on rare occasions, for security reasons, both roles may be carried out by the same person. Where specific, specialist units, particularly those involved in sensitive work, have undertaken streamlining to ensure better application of the principles of this code, these will generally be considered to be exceptional cases. One person may, in separate applications, carry out the roles of either the SPoC or the designated senior officer, or the roles of SPoC or the Applicant.

---

[23] See chapter 11 for further details of data protection safeguards.

4.39 The same person must never be both the applicant and the designated senior officer. Clearly, therefore, the same person should never be an applicant, a designated senior officer and a SPoC.

4.40 Any conduct to determine the CSP that holds, or may hold, specific communications data is not conduct to which the provisions of Part 3 apply. This includes, for example, establishing from information available to the public or, where necessary, from a service provider which provider makes available a specific service, such as a particular telephone number or an IP address.

4.41 Similarly Part 3 does not apply to any conduct by a public authority to obtain publicly or commercially available communications data. A Part 3 authorisation is not mandatory to obtain reference data[24], such as mobile phone mast locations, from a CSP as there is no intrusion with an individual's human rights. However, some reference data, such a details of Wi-Fi hotspots, may be commercially sensitive and a Part 3 authorisation can be sought by a public authority seeking to obtain this data from a CSP. Given the training undertaken by a SPoC and the on-going nature of a SPoCs engagement with CSPs, it is good practice to engage the SPoC to liaise with the CSP on such requests.

Exceptional circumstances

4.42 Section 73 provides for an authorisation to be granted without consultation with the SPoC in exceptional circumstances, which are limited to:

- The interests of national security; or
- Imminent threat to life or another emergency.

4.43 This provision does not absolve a public authority of the requirement to provide adequate SPoC cover for their investigative needs. The provision recognises that there may be some circumstances where, despite the best efforts of the public authority concerned, a SPOC is suddenly unavailable due, for example, to ill health. It is important that in such rare circumstances requests for communications data can be made in certain limited situations.

4.44 Organisations which are likely to deal with such cases should limit the risk that a SPoC is unavailable by entering into collaboration agreements where appropriate to do so.

4.45 There is a requirement to ensure that, in those cases where a SPoC is not available, the authenticity of the request can be or has been verified by the CSP. It is the responsibility of the public authority that considers such a process may be required to ensure that such a mechanism is in place.

4.46 In such cases the authorisation should record the reasons why SPoC coverage is not possible.

[24] See paragraph 2.24 for further information on reference data.

4.47 In all circumstances where public authorities do not consult a SPoC before an authorisation is granted, the senior responsible officer must notify the Commissioner of circumstances and reasons at the next inspection or as otherwise required by the Commissioner. CSPs should also record such instances and make these records available to the Commissioner on request. The details of the public authorities and the reasons such measures are being undertaken may be published and included in the Commissioner's report.

The senior responsible officer

4.48 Within every relevant public authority there should be a senior responsible officer. The senior responsible officer will be a person holding the office, rank or position of a designated senior officer within the public authority who may authorise access to communications data. The senior responsible officer is responsible for:

- The integrity of the process in place within the public authority to acquire communications data;
- Compliance with Part 3 of the Act and with this code;
- Oversight of the reporting of errors to the Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Commissioner's inspectors when they conduct their inspections; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the Commissioner.

Authorisations

4.49 An authorisation provides for persons within a public authority to engage in conduct, relating to a postal service or telecommunications system or data derived from such a telecommunication system, to obtain communications data. The following types of conduct may be authorised:

- Conduct to acquire communications data - which may include the public authority obtaining communications data themselves or asking any person believed to be in possession of or capable of obtaining the communications data to obtain and disclose it; or
- The issuing of a notice - allowing the public authority to require by a notice a telecommunications operator to obtain and disclose the required data.

4.50 An authorisation of conduct to acquire communications data may be appropriate where, for example:

- A CSP is not capable of obtaining or disclosing the communications data[25];
- There is an agreement in place between a public authority and a CSP relating to appropriate mechanisms for disclosure of communications data - in order to facilitate the secure and swift disclosure of communications data many CSPs have systems in place to ensure accurate and timely acquisition to communications data, while maintaining security and an audit trail;
- Where the data can be acquired directly from a telecommunication system and the activity does not constitute interception or equipment interference; or
- A designated senior officer considers there is a requirement to identify a person to whom a service is provided but a CSP has yet to be conclusively determined as the holder of the communications data.

4.51 An authorisation to issue a notice may be appropriate where a CSP is known to be capable of obtaining or disclosing the communications data (for further detail see paragraphs 4.67- 4.83).

4.52 Such an authorisation is not served upon a CSP, although there may be circumstances where a CSP may require or may be given an assurance that conduct being, or to be, undertaken is lawful. That assurance may be given by disclosing details of the authorisation or the authorisation itself. Where details of an authorisation are provided to a CSP in writing, electronically or orally, those details must additionally specify the manner in which the data should be disclosed and, where appropriate, provide an indication of any urgency or time within which the data need to be obtained.

4.53 Any designated senior officer in a public authority may only authorise persons working in the same public authority, or an authority which is a subscribing authority under a collaboration agreement, to engage in specific conduct, such as requesting the data via secure auditable communications data acquisition systems. This will normally be the public authority's or supplying authority's SPoC, though local authorities must now use the SPoC provided by the National Anti-Fraud Network (see chapter 6 for more details).

4.54 The decision of a designated senior officer whether to grant an authorisation shall be based upon information presented to them in an application.

4.55 Where an authorisation is granted under section 58(1)(b)(ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, the designated senior officer must be clear that it is also required for one of the purposes falling within section 58(7) and the application is proportionate to what is sought to be achieved.

4.56 An authorisation of conduct to acquire communications data must:

- Describe the conduct which is authorised and describe the communications data to be acquired by that conduct specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);

[25] Where possible, this assessment will be based upon information provided by the CSP.

- Specify the purpose for which the conduct is authorised, by reference to a statutory purpose under section 58(7) of the Act;
- Specify the office, rank or position held by the designated senior officer granting the authorisation. The name (or designation) of the designated senior officer granting the authorisation should also be recorded;
- Record the date and, when appropriate to do so, the time when the authorisation was granted by the designated senior officer;
- Confirm in writing that the designated senior officer has consulted a SPoC on this application;
- Specify where the communications data is to be obtained and disclosed by use of the request filter;
- If engaging the request filter, specify whether the processing of data (and its temporary retention for that purpose) is authorised and, if so, provide a description of the data that may be processed and the type or nature of processing to be performed (e.g. geographic correlation, IP address resolution);
- If engaging the request filter or requesting ICRs, specify whether any threshold for the number of results returned is set which would prevent any portion of records being disclosed;
- Where data is being sought from a CSP, specify whether the CSP may inform the subject(s) of the fact that an application has been made for their data; and
- Include a unique reference number.

4.57 In addition, an authorisation[26] to issue a notice must:

- Specify the operator to whom the notice applies and the nature of requirements to be imposed;
- Specify or describe the person(s) to whom the data is to be, or may be, disclosed or how to identify such person(s);
- Confirm whether a CSP may disclose the existence of this requirement, or any related pursuant request, to a customer or other individual;
- Specify whether the CSP may inform the subject(s) of the fact that an application has been made for their data; and
- Include a unique reference number and identify the public authority.

4.58 The original or a copy of the authorisation must be retained by the SPoC.

[26] Where the grant of an authorisation is recorded separately from the relevant application they should be cross-referenced to each other.

4.59 SPoCs and applicants should be mindful, when drafting authorisations within the meaning of section 58 of the Act, to ensure where possible the description of the required data corresponds with the way in which the CSP processes, retains and retrieves its data for lawful disclosure. CSPs cannot necessarily or reasonably edit or adapt their systems to take account of every possible variation of what may be specified in authorisations, particularly via communications data acquisition systems[27].

4.60 Requirements to identify a person to whom a service is, or has been, provided – for example telephone number subscriber checks – account for the vast majority of communications data disclosures. As a consequence of these requirements, some CSPs permit the lawful acquisition of this data by SPoCs, via secure auditable communications data acquisition systems. Where a SPoC has been authorised to engage in conduct to obtain details of a person to whom a service has been provided and concludes that data is held by a CSP from which it cannot be acquired directly, the SPoC may provide the CSP with details of the authorisation granted by the designated senior officer in order to seek disclosure of the required data.

4.61 It will often be appropriate to undertake the acquisition of entity data before obtaining related events data to confirm information within the investigation or operation.

4.62 However, where there is sufficient information within the investigation or operation to justify an application to obtain events data in the first instance, this may be undertaken. For example, in circumstances where:

- A victim reports receiving nuisance or threatening telephone calls or messages;
- A person who is subject of an investigation or operation is identified from high-grade intelligence to be using a specific communication service;
- A victim, a witness or a person who is subject of an investigation or operation has used a public payphone[28];
- A person who is subject of an investigation or operation is identified during an investigation (such as a kidnap) or from detailed analysis of data available to the investigator to be using a specific communication service;
- A mobile telephone is lawfully seized and communications data is to be acquired relating to either or both the device or its SIM card(s);
- A witness presents certain facts and there is a need to corroborate or research the veracity of those, such as to confirm the time of an incident they have witnessed; or
- An investigation of the allocation of IP addresses is needed to determine relevant subscriber information.

4.63 Where the acquisition of the entity data is required to assist an investigation or operation or for evidential purposes, that requirement can be included on an application for events data.

---

[27] The College of Policing Knowledge and Engagement Team (KET) (ketadmin@college.pnn.police.uk) can provide advice to SPoCs on how best to ensure up-to-date knowledge of data types.

[28] The telephone number and address of a public payphone is normally displayed beside it to assist persons making emergency calls to give their location to the emergency operator.

4.64 At the time of granting an authorisation of conduct to acquire communications data or to issue a notice in order to obtain specific events data, a designated senior officer may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of specific entity data relating to the events data to be obtained. This is relevant where there is a necessary and proportionate requirement to identify with whom a person has been in communication, for example:

- To identify with whom a victim was in contact, within a specified period, prior to their murder;
- To identify, where the target of an investigation or operation has been observed to make several calls from a public pay phone, the recipient of those calls;
- To identify a person making unlawful and unwarranted demands (as in the case of kidnap, extortion and blackmail demands and threats of violence); or
- Where a victim or a witness has identified a specific communication or communications and corroboration of facts may reveal a potential offender or other witness.

4.65 At the time of granting an authorisation of conduct to acquire communications data or to issue a notice in order to obtain specific events data, a designated senior officer may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of other events data. This is relevant where there is a necessary and proportionate requirement to identify a person from the events data to be acquired, and the means to do so requires the CSP or another CSP to query their events data information, for example:

- The CSP does not collect information about the customer within their customer information system but retains it in its original form as events data (such as a MAC or IMEI or an IP address); or
- Where evidence or intelligence indicates there are several CSPs involved in routing a communication and there is a requirement to establish the recipient of the communication.

4.66 It is the duty of the senior responsible officer to ensure that the designated senior officer, applicant or other person makes available to the SPoC such information as the senior responsible officer thinks necessary to ensure the integrity of any requirements for the acquisition of entity data to be obtained directly upon the acquisition or disclosure of any events data, and their compliance with Part 3 and with this code[29].

Notices

4.67 The giving of a notice is appropriate where a CSP is able to retrieve or obtain specific data, and to disclose that data, and the relevant authorisation has been granted. A notice may require a CSP to obtain any communications data, if that data is not already in its possession.

[29] Ordinarily the applicant or other person within the investigation or operation will prepare a schedule of data, for example telephone numbers, to enable the SPoC to undertake the acquisition of subscriber information. The schedule will include details of the person who prepared it, cross reference it to the relevant notice or authorisation and specify the events data from which the data are derived.

4.68 The decision of a designated senior officer whether to authorise the issuing of a notice shall be based on information presented to them in an application.

4.69 Once the designated senior officer has authorised that a notice should be given, it will be served upon a CSP in writing[30] or, in an urgent situation, communicated to the CSP orally.

4.70 The notice should contain enough information to allow the CSP to comply with the requirements of the notice.

4.71 A notice must:

- Be given in writing or, if not, in a manner that produces a record, within the public authority, of its having been given;
- Describe the communications data to be obtained or disclosed under the notice specifying, where relevant, any historic or future date(s)and, where appropriate, time period(s);
- Specify the requirements being imposed and the telecommunications operator on whom the requirements are being imposed;
- Where appropriate, provide an indication of any urgency or time within which the CSP is requested to comply with the requirements of the notice;
- Specify the purpose for which the notice has been given, by reference to a statutory purpose under section 58(7) of the Act;
- Include an explanation that compliance with the notice is a requirement of the Act unless the notice is cancelled. A CSP which has not complied before the period of validity for the authorisation expires is still required to comply. The notice should contain sufficient information including the contact details of the SPoC to enable a CSP to confirm the notice is authentic and lawful;
- Specify the manner in which the data should be disclosed and specify or describe the person(s) to whom the data is to be, or may be, disclosed or how to identify such person(s);
- Specify whether the data to be disclosed will pass through the filtering arrangements;
- Specify whether any threshold for the number of results returned is set which would prevent any portion of records being disclosed;
- Specify the office, rank or position held by the designated senior officer giving the notice. The name (or designation) of the designated senior officer giving the notice should also be recorded;
- Record the date and, when appropriate to do so, the time when the notice was given by the designated senior officer;
- Specify whether the CSP may inform the subject(s) of the fact that an application has been made for their data; and
- Include a unique reference number and identify the public authority[31].

[30] 'In writing' can include, but is not limited to, letter, fax, email, or via a secure portal operated by the CSP.

4.72 The original or a copy of the notice must be retained by the SPoC.

4.73 A CSP is not required to do anything under a notice which it is not reasonably practicable for it to do[32].

4.74 In giving notice a designated senior officer may only require a CSP to disclose the communications data to the designated senior officer or to a specified person working within the same public authority or an authority which is a subscribing authority under a collaboration agreement. This will normally be the public authority's SPoC.

4.75 Ordinarily the CSP should disclose, in writing or electronically, the communications data to which a notice relates not later than the end of the period of ten working days from the date the notice is served upon the CSP.

4.76 If a CSP, having been given a notice, believes that in future another CSP is better placed to respond, they should approach the authority to inform them of their view after disclosing the relevant data that they hold.

Urgent oral giving of notice or grant of authorisation

4.77 In exceptionally urgent circumstances[33], an application for the grant of an authorisation may be made by an applicant, approved by a designated senior officer and either notice given to a CSP or an authorisation granted orally. Circumstances in which an oral notice or authorisation may be appropriate include:

- An immediate threat of loss of human life, or for the protection of human life, such that a person's life might be endangered if the application procedure were undertaken in writing from the outset - this may include those situations where, for example there is serious concern for the welfare of a vulnerable person including children at imminent risk of being abused or otherwise harmed;
- an exceptionally urgent operational requirement where, within no more than 48 hours of the notice being given or the authorisation being granted orally, the acquisition of communications data will directly assist the prevention or detection of the commission of a serious crime[34] and the making of arrests or the seizure of illicit material, and where that operational opportunity will be lost if the application procedure is undertaken in writing from the outset; or
- A credible and immediate threat to national security or a time-critical and unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost, if the application procedure were undertaken in writing from the outset.

---

31 This can be a code or an abbreviation. It could be that part of a public authority's name which appears in its e-mail address. For police services it will be appropriate to use the Police National Computer (PNC) force coding.

32 See section 63(3) of the Act. SPoCs, designated senior officers or CSPs may contact the KET if they require further advice on what is reasonably practicable in a particular circumstance.

33 There is a general undertaking by CSPs to respond outside of normal office hours where there is an immediate threat to life.

34 See section 239(1) of the Act.

4.78 The use of urgent oral process must be justified for each application within an investigation or operation. The fact that any part of an investigation or operation is undertaken urgently must not be taken to mean that all requirements to obtain communications data in connection with that investigation or operation be undertaken using the urgent oral process. It must be clear in each case why it was not possible, in the circumstances, to use the standard, written process.

4.79 When, in a matter of urgency, a designated senior officer decides, having consulted the SPoC, that the oral giving of a notice or grant of an authorisation is appropriate, that notice should be given or the authorised conduct undertaken as soon as practicable after the making of that decision.

4.80 Particular care must be given to the use of the urgent oral process. When authorisation is given orally, the SPoC, when relaying service of the oral authorisation to the CSP, must make a note of the time, provide a unique reference number for the notice, provide the name (or designation) of the designated senior officer and the name and contact details of the SPoC and, if required by the CSP, their authentication identifier[35]. Where telephone numbers (or other identifiers) are being relayed, the relevant number must be read twice and repeated back by the CSP to confirm the correct details have been taken.

4.81 Written notice must be given to the CSP retrospectively within one working day[36] of the oral authorisation being given. Failure to do so will constitute an error which may be reported to the Commissioner by the CSP and must be recorded by the public authority (see the section on errors in chapter 21, Keeping of records, for more details).

4.82 After the period of urgency[37], a separate written process must be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the SPoC shall collate details or copies of control room or other operational logs which provide contemporaneous records of the consideration given to the acquisition of data, decision(s) made by the designated senior officer and the actions taken in respect of the decision(s).

4.83 In all cases where urgent oral notice is given or authorisation granted, an explanation of why the urgent process was undertaken must be recorded.

---

[35] At the time of writing, this is the SPoC PIN, see footnote 19.

[36] Working day means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday in any part of the United Kingdom.

[37] In some instances where life is at risk, for example in kidnap investigations, the period of urgency may be prolonged.

5 Duration, renewals and cancellations

Duration of authorisations and notices

5.1 An authorisation becomes valid on the date upon which authorisation is granted. It is then valid for a maximum of one month[38]. This means the conduct authorised should have been commenced or the notice served within that month.

5.2 Any notice issued under an authorisation remains in force until complied with or until the authorisation under which it was issued is cancelled (see paragraph 5.9).

5.3 All authorisations should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s)[39]. Any period should be clearly indicated in the authorisation. The start date and end date should be given, and where a precise start and end time are relevant these must be specified[40]. Where the data to be acquired or disclosed is specified as 'current', the relevant date should be taken to be the date on which the authorisation was granted by the designated senior officer. There can be circumstances when the relevant date or period cannot be specified other than 'the last transaction' or 'the most recent use of the service'.

5.4 Where an authorisation relates to the acquisition or obtaining of specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date upon which the authorisation was granted.

5.5 Designated senior officers should specify the shortest possible period of time for any authorisation. To do otherwise would impact on the proportionality of the authorisation and impose an unnecessary burden upon the relevant CSP(s).

Renewal of authorisations and notices

5.6 Any valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation. A renewed authorisation takes effect upon the expiry of the authorisation it is renewing.

5.7 Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasoning for seeking renewal should be set out by an applicant in an addendum to the application upon which the authorisation being renewed was granted.

---

[38] Throughout this code, a month means a period of time extending from a date in one calendar month to the date one day before the corresponding or nearest date in the following month. For example, a month beginning on 7 June ends on 6 July; a month beginning on 30 January ends on 28 February or 29 February in a leap year.

[39] For example, details of events data on a specific date or for a specific period or the details of a subscriber on a specific date or for a specific period.

[40] In the case of IP data, any timings should include an explicit indication of which time zone applies to those timings.

5.8 Where a designated senior officer is granting a further authorisation to renew an earlier authorisation[41], the designated senior officer should:

- Have considered the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated; and
- Record the date and, when appropriate to do so, the time when the authorisation is renewed.

Cancellation of authorisations and notices

5.9 A designated senior officer who has granted an authorisation under section 58(2) of the Act must cancel it if, at any time after the granting of the authorisaitone[42], it is no longer necessary for a statutory purpose or the conduct required by the authorisation is no longer proportionate to what was sought to be achieved. An authorisation may otherwise be cancelled at any time.

5.10 It may be the case that it is the SPoC or the applicant who is first aware that the authorisation is no longer necessary or proportionate. In such cases the SPoC (having been contacted by the applicant, where appropriate) may cease the authorised conduct, and then inform the designated senior officer who granted the authorisation

5.11 A notice issued under an authorisation (and any requirement imposed by a notice) is cancelled if the authorisation is cancelled but is not affected by the authorisation ceasing to have effect at the end of one month period of validity. Reporting the cancellation of a notice to a CSP should be undertaken by the designated senior officer directly or, on that person's behalf, by the public authority's SPoC. Where human rights considerations are such that a notice should be cancelled with immediate effect the designated senior officer or the SPoC will notify the CSP[43].

5.12 Cancellation of a notice reported to a CSP must:

- Identify, by reference to its unique reference number, the notice being cancelled; and
- Record the date and, when appropriate to do so, the time when the notice was cancelled.

5.13 In cases where the SPoC has initiated the cancellation of a notice and reported the cancellation to the CSP, the designated senior officer must confirm the decision for the SPoC either in writing or, if not, in a manner that produces a record of the notice having been cancelled by the designated senior officer. Where the designated senior officer who gave the notice to the CSP is no longer available, this duty should fall on a person who has temporarily or permanently taken over the role of the designated senior officer.

---

41 This can include an authorisation that has been renewed previously.

42 This can include a renewed authorisation.

43 If the authorisation being cancelled relates to an urgent operational situation that has been resolved, or has changed, it may be appropriate for the senior officer dealing with the situation, on the ground or in a control room, to notify the CSP (or arrange for their notification) that the notice imposed under an authorisation is cancelled where that person has the earliest opportunity to do so.

5.14

5.15 Cancellation of an authorisation should:

- Identify, by reference to its unique reference number, the authorisation being withdrawn;
- Record the date and, when appropriate to do so, the time when the authorisation was cancelled; and
- Record the name and the office, rank or position held by the designated senior officer informed of the withdrawal of the authorisation.

5.16 When it is appropriate to do so, a CSP should be advised of the cancellation of an authorisation, for example where details of an authorisation have been disclosed to a CSP.

6 Further restrictions and requirements in relation to applications

Communications data involving certain professions

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

6.2 However the degree of interference with an individual's rights and freedoms may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament[44], or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.

6.3 Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken by designated senior officers when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application.

6.4 Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That such an application has been made must be recorded (see chapter 21 on keeping of records for more details), including recording the profession, and, at the next inspection, such applications should be flagged to the Commissioner.

Applications for communications data relating to journalists and their sources

6.5 Issues surrounding the infringement of the right to freedom of expression may arise where an application is made for the communications data ofan identified or suspected journalist, an identified source or a suspected source of journalistic information and particularly, but not solely, where that application is for the purpose of identifying or confirming the identity or role of an individual as a journalist's source.

6.6 There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously.

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

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

6.8 An assessment of whether someone is a journalist (for the purposes of the Act) should be made on all the facts and circumstances available at that time. Consideration should be given, in particular, to the frequency of an individual's relevant activities, the level of professional rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest.

6.9 Where a designated senior officer is unclear as to whether an individual may be considered to be a journalist they should seek advice before authorising a relevant application (see para 6.15).

6.10 Applications for communications data in relation to journalists and their sources may still be made but applicants and designated senior officers will want to take particular care in considering such applications. To ensure that an application made to acquire communications data relating to a journalist or source is lawful it is crucial that public authorities apply correctly the process set out in this chapter.

6.11 The acquisition of communications data under Part 3 of the Act will be a justifiable interference with an individual's human rights under Articles 8 (right to respect for private and family life) and, in certain circumstances, 10 (freedom of expression) of the European Convention on Human Rights only if the conduct being authorised or required to take place is necessary, proportionate and in accordance with law.

6.12 Where an application is intended to identify or confirm the identity or role of an individual as a source of journalistic information judicial approval of the authorisation must be sought prior to the acquisition of the communications data taking place, other than where an exception applies. Where an application is not intended to identify or confirm the identity or role of an individual as a source of journalistic information judicial approval is not required but care should be taken.

6.13 Communications data alone may not be sufficient to identify a source - consequential action and other information is likely to be required. Identifying communications addresses does not in itself provide sufficient information to determine the nature of a relationship. However, where such requests are made with the intention that the information obtained will be used as part of an assessment of the identity of a source, this will require judicial commissioner authorisation.

6.14 The process for and guidance on both scenarios is set out in the following paragraphs.

6.15 Where appropriate public authorities should seek advice on the application of these provisions from the Home Office, the Investigatory Powers Commissioner and their own legal team. In addition, where an application may be considered novel or contentious public authorities should refer the matter to a Judicial Commissioner to review before deciding whether to authorise the application (see paras 6.34 onwards).

Applications to identify or confirm the identity or role of an individual as a source of journalistic information

6.16 Public authorities will, in very limited circumstances, have a legitimate need to acquire communications data to identify or confirm the identity or role of an individual as a journalist's source. In such circumstances issues surrounding the infringement of the right to freedom of expression are likely to arise. Public authorities must consider whether there is another overriding public interest which justifies any interference with this right.

6.17 Where a designated senior officer has granted an authorisation for this purpose in circumstances other than in relation to an immediate threat to life (see below) the authorisation will not take effect until such time as a Judicial Commissioner has approved it under section 74 of the Act.

6.18 In deciding whether to approve an authorisation to identify or confirm the role of an individual as a journalistic source a Judicial Commissioner must, among other matters, have regard to the public interest in protecting a source of journalistic information and consider that there is another overriding public interest before approving an authorisation.

6.19 In considering whether an application is being made for the purpose of identifying or confirming the identity or the role of an individual as a journalist's source, public authorities should pay particular consideration to applications relating to communications addresses of:

- persons identified as or suspected to be a source;
- persons identified as or suspected to be acting as an intermediary between a journalist and an identified or suspected source; and
- person identified as or suspected to be a journalist.

6.20 In addition to applications specifically intended to identify a journalist's source, the acquisition of communications data to confirm existing understanding or corroborate other evidence of the identity of, or role of an individual as, a journalist's source requires judicial authorisation.

6.21 The requirement for judicial authorisation applies to an authorisation made for the purpose of identifying or confirming any identifying characteristic of a source, not solely their name. For instance, in certain circumstances it may not be the name of a source that is being sought but other identifying characteristics such as their home location or occupation.

6.22 Designated senior officers should apply careful consideration before authorising the acquisition of communications data to identify or confirm who within a public authority may have leaked information to the media. Such an application should only be made where it is considered that there is a public interest in making such an application which overrides the public interest in source protection. Judicial authorisation is required. This includes situations where the passing of any information may in itself constitute a crime.

6.23 In addition to the requirements detailed in chapter 4, an application to acquire communications data for the purpose of identifying or confirming the role of an individual as a source should give special consideration to necessity and proportionality and specifically draw attention to the following matters:

- **Potential infringements of rights**: The existence of any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and freedom of expression.

- **Public interest in source protection**: Consideration of whether the intrusion is justified, giving proper consideration to whether the public interest is best served by the application. The application should consider properly whether the suspected conduct is of a sufficiently serious nature for rights to freedom of expression to be interfered with.

- **Collateral intrusion**: As well as consideration of the rights of the individual under investigation, consideration should also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. Any potential for unintended consequences of such applications should be considered.

6.24 It will not be sufficient to simply state, without any further detail on how the matters apply in the case and any mitigations put in place that the matters have been appropriately considered.

6.25 Each authority must keep a central record of all occasions when such an application has been made, including a record of the considerations undertaken (see chapter 21 on keeping of records for more details). At the next inspection, such applications should be specifically flagged to the Commissioner.

6.26 An authorisation made for the purpose of identifying or confirming the role of an individual as a journalist's source cannot take effect until such time as a Judicial Commissioner has approved it, except where an authorisation is not required due to an imminent threat to life

Threat to life exception

6.27 In very limited circumstances an authorisation made for the purpose of identifying or confirming the identity or role of an individual as a journalist's source will not require judicial approval. If, and only if, there is believed to be an immediate threat of loss of human life, such that a person's life might be endangered by the delay inherent in the process of judicial authorisation, law enforcement agencies may continue to use the existing internal authorisation process under the Act.

6.28 Examples of situations in which judicial approval may not be required due to an immediate threat to loss of human life include:

- a warning of an imminent terrorist incident being telephoned to a journalist or newspaper office;

- a journalist conducting an investigation which includes a significant element of personal danger who has not checked in with his office at the agreed time; or

- a source contacting a journalist to reveal their intention to commit suicide.

6.29 Such applications must be notified to the Commissioner as soon as reasonably practicable, as agreed with the Commissioner.

6.30 If additional communications data is later sought for the purpose of identifying or confirming the identity or the role of an individual as a journalist's source as part of the same investigation, but where a threat to life no longer exists, judicial approval should be sought.

Applications relating to journalists which are *not* to identify or confirm the identity or role of an individual as a source of journalistic information

6.31 The requirement for judicial oversight does not apply where applications are made for the communications data of those known or suspected to be journalists or sources but where the application is not to identify or confirm the role of an individual as a source of journalistic information.

6.32 The following paragraphs provide examples of when an application relating to a journalist or their source may be considered not to be for the purpose of identifying or confirming the role of an individual as a journalist's source. In each case, public authorities should apply their own assessment to the specific circumstances of the case and identify whether there is any potential additional infringement of rights or intrusion to be considered, including whether the application should be considered novel or contentious (see para 6.34).

- Where the journalist is a victim of crime and it is clear that their profession and sources are not relevant to the investigation, judicial approval may not be required.

- Where an identified source or suspected source is a victim of crime and it is clear that their role as a source is not relevant to the investigation, judicial approval may not be required.

- Where a journalist, identified source, or suspected source is a witness or other by-stander in an investigation not related to their roles as journalist or source and a communications data application is made to discount them from the investigation, judicial approval may not be required.

- Where the journalist, identified source, or suspected source is suspected of committing a crime, judicial approval may not be required in all circumstances:

    - For instance, where a journalist is suspected of committing a crime and it is clear that their profession and sources are not relevant to the investigation, judicial approval may not be required.

    - Additionally, it may be necessary to acquire the communications data of a known criminal under investigation who is also a source. Where a

journalist-source relationship is already confirmed and the individual's role as a source is not relevant to the investigation, judicial approval may not be required.

- Where an individual on the witness protection programme is concerned that an unsolicited caller is a journalist, or other individual, hoping to sell a story about the individual's new identity, judicial approval may not be required.

- Where an investigation is conducted to prove criminal conspiracy between a journalist and their source, and the journalist-source relationship is already confirmed, judicial approval may not be required in all circumstances. For example, where specific facts about the timing or location of communications between the two individuals must be confirmed to prove the criminal conspiracy, judicial approval may not be required.

6.33 An application for communications data relating to a known or suspected journalist or a known or suspected source, which is not to identify or confirm the identity or role of an individual as a journalist's source, may still have an unusual degree of sensitivity attached to it. Where this is the case the application should be considered potentially contentious and referred to the Judicial Commissioner for review.

6.34 Applications which should be considered to fall into this category and should therefore be referred to the Judicial Commissioner include, but are not limited to, applications for communications data of a journalist or their source which are not to identify or confirm the identity or role of an individual as a journalistic source and:

- Will likely result in the incidental and unintended identification or confirmation of a source (collateral intrusion into journalist sources) yet may still be justified; or

- Relate to an investigation involving whistle-blowing or the leaking of documents or information to the media. An application for the purpose of limiting reputational damage would not meet a statutory purpose and so would not be considered lawful.

6.35 An example of collateral intrusion into a journalist's source may be where:

- subscriber checks are requested for all communications addresses in contact with a journalist over a period of time because, for instance, they are a victim of a serious crime; and

- those checks are not for the purpose of identifying or confirming a source; and

- information is already known about a source run by that journalist which will unavoidably result in the identification of that source if subscriber checks are obtained.

6.36 Particular care should therefore be taken to ensure that the application considers whether the intrusion is justified, giving proper consideration to the public interest. As well as consideration of the rights of the individual under investigation, consideration should also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. Any potential for unintended consequences of such applications should be considered.

Novel and contentious acquisition

6.37 In recognition of the capacity of modern communications data to produce insights of a highly personal nature, where it is considered that a communications data application is novel or contentious, the senior responsible officer must refer the matter to a Judicial Commissioner for advice before deciding whether to authorise the application. A referral to the Judicial Commissioner may relate to a single application or to an issue of principal arising in an application.

6.38 Where appropriate the senior responsible officer should discuss with the Commissioner particular circumstances which might cause a case to be considered novel and contentious for that public authority. An application for communications data might be considered novel and contentious for one public authority but not another.

6.39 The following examples might be considered novel or contentious:

- New technical methods of acquisition;
- New types of communications data;
- Applications which might result in an unusual amount of collateral intrusion but still be considered proportionate; and
- Where there might be unusual sensitivity attached to the application regarding the nature of the target.

6.40 For guidance on how applications for communications data relating to a journalist or their source may be considered novel or contentious, please see para 6.34.

6.41 Where the designated senior officer or senior responsible officer is in any doubt regarding whether an application is novel or contentious they should consult the Commissioner before deciding whether to seek advice on such a case.

6.42 In urgent cases, such as threat to life or the interests of national security in a particular investigation, it may not be possible to seek the opinion of the Commissioner in advance of making an application for the data. In such circumstances the public authority should seek retrospective advice as soon as possible and take this into account in future applications of a similar nature.

6.43 The public authority must record the views of the Judicial Commissioner and where the designated senior officer proceeds against the recommendation of the Judicial Commissioner must give his reasons for doing so.

6.44 The views of the Judicial Commissioner on such cases should be recorded and may be shared between public authorities to inform consideration of future applications.

Public authority collaboration agreements

6.45 Any public authority may participate in a collaboration agreement, by which the designated senior officer and other officers of the supplying authority are put at the disposal of the subscribing authority. In practice, the subscribing authority will most commonly make use of a partner's designated senior officer and SPoC. A public authority may be directed to enter into such an agreement by the Secretary of State. All local authorities must make applications through a SPoC at the National Anti-Fraud Network ('NAFN') (see paragraph 6.51).

6.46 Before entering into a collaboration agreement, all parties to the agreement should consider whether:

- Sufficient alignment exists between the parties to allow the supplying authority to meet the specific needs of the subscribing authority, for instance provision of out-of-hours services or specific security clearances;
- The supplying authority is sufficiently familiar with the subscribing authority's role to be able to provide relevant expertise; and
- The length of time the collaboration agreement will last for, for instance whether the agreement is just for the duration of a particular operational requirement.

6.47 When deciding whether to direct a public authority to enter into a collaboration agreement the Secretary of State will consider:

- The issues identified in paragraph 6.46;
- The number and nature of authorisations made by a public authority; and
- The nature and function of the public authority concerned.

6.48 In granting authorisations on behalf of the subscribing authority, the designated senior officer at the supplying authority must ensure that in accordance with the provisions under Schedule 4 of the Act:

- Authorisations are only granted to the subscribing authority for the purposes for which that authority may acquire communications data; and
- The designated senior officer holds the relevant minimum rank or position detailed for the subscribing authority

6.49 Any collaboration agreement between public authorities must be undertaken in writing or, if not, in a manner that produces a record within the relevant public authorities. This agreement, or the fact of its existence, must then be published along with any other details considered appropriate and the Commissioner notified.

Local authority procedures

6.50 NAFN provides shared SPoC services to local authorities. Local government legislation allows for NAFN to act on behalf of local authorities within England and Wales, Scotland and Northern Ireland for certain functions[45].

6.51 In accordance with section 71 all local authorities who wish to acquire communications data under the Act are required to become members of NAFN and use their shared SPoC services. This means that applicants within local authorities are required to consult a NAFN SPoC throughout the authorisation process, including before referring the case to a designated senior officer for approval. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to applicants and designated senior officers ensuring the local authority acts in an informed and lawful manner.

6.52 In addition, local authority applications for communications data require judicial approval under section 72 of the Act. Judicial approval must be requested once all the internal authorisation processes have been completed, including consultation with a NAFN SPoC, but before the SPoC requests the data from the CSP. In England, Wales and Northern Ireland the authorisation must be provided by a magistrate; in Scotland a sheriff or summary sheriff.

6.53 The local authority, rather than NAFN, is responsible for submitting the application for judicial authorisation. It is for the local authority to decide on the most appropriate representative to present their application to the magistrate or sheriff. The judicial application must include relevant documentation, including the original Act authorisation or notice. Once the case has been heard, the magistrate or sheriff will complete a judicial order outlining their decision. Should authorisation be granted, the local authority will provide the judicial order to the NAFN SPoC.

6.54 Where a local authority seeks communications data for the purposes of identifying or confirming a journalistic source the requirement to seek local magistrate approval under section 72 does not apply. Instead the local authority must apply to the Judicial Commissioner for approval of the authorisation under section 74.

6.55 A local authority may not grant an authorisation requiring the processing or disclosure of internet connection records for any purpose (see chapter 7).

[45] The Local Government Act 1972; Local Government Act (Scotland) 1973; and Local Government Act (Northern Ireland) 2014.

7 Considerations in relation to the acquisition of internet data

Internet connection records

7.1 In addition, under certain circumstances, a designated senior officer may grant an authorisation to obtain data which constitutes or requires the processing or disclosure of an internet connection record (ICR) (see paragraph 2.62 for the definition of an ICR). Subject to paragraph 2.28 any application that involves the disclosure of ICRs must be authorised as events data.

7.2 All existing requirements regarding necessity and proportionality for authorisations to obtain communications data also apply to the acquisition of ICRs. However, in addition, particular care must be taken by designated senior officers when considering such applications, including additional consideration of the proportionality of the application in relation to the level of processing, where known, and disclosure involved.

7.3 Section 59 of the Act recognises the additional sensitivities associated with ICRs and restricts public authority access accordingly. A public authority can therefore only require the disclosure or processing of internet connection records for the purpose of identifying:

- The sender of an online communication (either the device or the person);
- The internet communications services[46] an individual is using, such as messaging applications;
- The internet services[47] an individual is using which wholly or mainly involve making available or acquiring material, whose possession is a crime – for example child abuse imagery or illicit drugs; or
- Other internet services an individual is using – for example to book travel or look at online mapping services.

7.4 An application to acquire ICRs may relate to one or more of these 'investigative purposes'.

7.5 The Act applies important restrictions when the statutory purpose for which ICRs are acquired is for the prevention and detection of crime. In these circumstances ICRs can only be acquired:

---

[46] An internet communication service is a service which provides for the communication between one or more persons over the internet and may include email services, internet telephony services and web forums.

[47] An internet service is a service provided over the internet. It includes internet communication services, websites and applications.

- for the prevention and detection of crime where the offence, or one of the offences, is one for which a person is capable of being sentenced to imprisonment for a term of 6 months or more;

- for the prevention and detection of any other crime which would fall within the definition of serious crime in section 239 of the Act, - i.e. offences involving the use of violence, conduct that results in substantial financial gain and conduct by a large number of people in pursuit of a common purpose;

- where the conduct is an offence which can only be committed by a corporate body – for example corporate manslaughter - where a penalty of imprisonment does not apply; and

- where the conduct concerned involves, as an integral part of it, the sending of a communication or a breach of a person's privacy - for example cyber bullying and harassment offences and offences which are themselves invasions of privacy such as data protection offences of unlawfully acquiring personal information.

7.6 The crime threshold does not apply to applications made for the investigative purposes of identifying the sender of an online communication (section 59(3)). Such applications will not result in the disclosure of a list of internet connection records as the service used will already be known. A CSP could be asked a number of different questions, for example who was using this IP address at date/time, which of your customers has accessed this server at date/time or which of your customers conducted an activity of concern on a known website at a known date or time. The material disclosed will thus take the form of an IP address and related entity data, where available (see identifying the sender of an online communication in the next section).

7.7 Applications may be made by the public authority for the purposes of identifying:

- The communications service used by an individual;

- Internet services used to access or make available illegal material; or

- What other internet services a person is using.

7.8 Such applications will require a CSP to disclose of a list of internet connection records covering a specific time period. This will include ICRs not directly relevant to the investigation. Given the scope for collateral intrusion the designated senior officer will therefore need to apply careful consideration to ensure this period is proportionate and no longer than necessary.

7.9 Occasions when a public authority might seek ICRs to identify an internet communications service being used include:

- To facilitate follow up with another communications provider in order to establish who a missing person was in contact with before their disappearance;

- Where a person is known to be communicating online but it is not known how; or

- To facilitate follow up with another communications provider in order to identify contacts of a suspect following the seizing of a communication device.

7.10 An ICR is unlikely to identify who a person has been communicating with online or when they have been communicating. In most cases it will simply identify the services which a person has accessed allowing further enquiries to be made of the relevant provider.

7.11 A public authority might seek ICRs in order to identify possible access to illegal information when seeking, for instance, to identify whether a person seen viewing illegal images has been accessing sites containing this information, to identify whether a person suspected of owning illegal weapons has been accessing illegal online market places or to identify which website a person has uploaded illegal images.

7.12 A public authority might seek ICRs in relation to internet services more generally when seeking, for instance, to identify how a person who is suspected of people trafficking is making travel arrangements or to identify any activity which may assist in locating a missing vulnerable person. Any services accessed by an individual may provide leads for public authorities to pursue in their investigation by identifying travel services, mapping applications or other relevant avenues to follow up.

7.13 A public authority may only examine internet connection records returned to them which do not directly relate to the purpose for which they were acquired (for example a record of access to a travel site returned in response to a request for communication services) where necessary and proportionate to do so for the purposes set out in section 58(7) of the Act. For further information see paragraphs 21.37 - 21.39 on excess data.

7.14 Local authorities are prohibited from seeking the processing or disclosure of ICRs for any purpose.

7.15 There may be circumstances where it is more appropriate for public authorities to utilise the alternative lawful powers available to them, such as interception or equipment interference warrants, to obtain information which is similar to, or includes, ICRs. The use of these powers will be subject to higher levels of authorisation, requiring a warrant to be issued by the Secretary of State and approved by a Judicial Commissioner. Before using such powers the relevant authority must consider whether a less intrusive means of collecting such data is appropriate.

Identifying the sender of an online communication

7.16 Internet Protocol Address Resolution (IPAR) is necessary to identify the sender of an online communication, where the public authority is in possession of an IP address related to a communication of interest and needs to determine the associated user(s). In the current technological environment this is often not a simple task and applications to acquire communications data for this purpose must consider the associated complexities.

7.17 In order to communicate on the internet a device must be allocated an IP address. A communication may be between two users, in which case the IP address will normally relate to their personal electronic device, between two servers in which case the IP addresses will relate to the equipment in question, or between a user's personal electronic device and a server for instance a user downloading material from a website. The IP address from which the communication originated is the source IP address, that by which it is received is the destination IP address.

7.18 In order to enable the CSP to resolve an IP address the public authority must provide a minimum of one source IP address and one date/time. To enable the identification of a person who initiated a communication, rather than the service used to send that communication this must be a source IP which relates to a user's personal device not a server.

7.19 However, where IP addresses are shared between network customers as is commonly the case, provision of just the source IP address and the time of the communications will often not be sufficient to resolve the address to an individual. Public authorities should therefore ensure they use any other data that is available to them with the application. For example, if there are more IP addresses and times which they believe relate to the same suspect then that data should also be provided to the CSP. This includes the following types of data where available:

- Source and destination port numbers, both public and private;
- User equipment identifiers;
- Account reference details; and
- Service identifiers or web domains.

7.20 Where public authorities need to resolve IP addresses, internet connection record data will often be the only additional data that is available. This is because they will already know the internet service that has been used to send the relevant communication which they are trying to resolve. For example, if someone posts a bomb threat to an online blog, the blog's access records will provide the police with both the source IP address allocated to the user who posted the threat, as well as the destination IP address of the blog server. The police should provide both these IP addresses, plus any other information the blog records provide such as ports used, to the CSP as this will increase the likelihood that the CSP will be able to accurately match these details to an individual.

7.21 Network implementation of network address translation and dynamic IP addressing means that an IP address may only be allocated to a particular user in conjunction with other users, and sometimes for an extremely short period of time, particularly where allocated to mobile devices. A request for IPAR data may therefore return a large data set to the public authority. As a designated senior officer will not know in advance how large that return will be, it is important to consider the proportionality and potential collateral intrusion of such applications.

7.22 In addition to the standard authorisation procedure for communications data applications the following additional steps should be taken:

- The applicant should consider what data is available to them and base their application on those elements of data which will enable the CSP to make the most accurate and proportionate return;

- The applicant should use as many relevant identifiers as are available to them in making their application, in order to ensure that the CSP may make the most accurate return. Where more than one IP address or more than one date / time is available, the public authority should consider resolving more than one to allow cross-correlation of data sets;

- The designated senior officer must take account of advice provided by the SPoC as to an appropriate strategy for the acquisition of IPAR data in each case;

- The designated senior officer must consider, in making an application, whether to specify that the CSP should only return the data where it can be linked to one individual or whether larger data sets may be returned. The designated senior officer may decide to accept returns of larger data sets only where the necessity and proportionality case is sufficiently strong and must detail their considerations of proportionality in the authorisation; and

- The designated senior officer must give consideration to where returns of incomplete data could lead to false positives or false negatives for an operation and how this might be mitigated through the use of corroborating evidence. As a greater number of communications services become available, it is no longer possible to obtain full visibility of an individual's communications. Whilst the data available might only identify one individual who meets the specified criteria, the provision of further data regarding other communications methods might identify further matches, thus rendering the initial result a 'false positive'. The likelihood of 'false negatives' where individuals are ruled out of a case because they did not appear in a particular data set should also be considered.

7.23 The same considerations will apply where the public authority does not have an IP address but wishes to determine the individual that carried out a certain action online.

8 Special rules on the granting of authorisations and giving of notices in specific matters of public interest

Sudden deaths, serious injuries, vulnerable and missing persons

8.1 There are circumstances when the police undertake enquiries in relation to specific matters of public interest where the disclosure of communications data may be necessary and proportionate. Section 58(7) of the Act specifies certain purposes for which the acquisition and disclosure of communications data may be necessary. These purposes assist the police in carrying out its functions. For example:

- Identifying any person who has died or who is unable to identify himself because of a physical or mental condition, other than as a result of crime (for example in the case of a natural disaster or an accident);
- Obtaining information about the reason for a person's death or condition;
- Locating and notifying next of kin following a sudden or unexpected death;
- Locating and notifying next of kin of a seriously injured person; and
- Locating and notifying the next of kin or responsible adult of a child or other vulnerable person where there is a concern for the child's or the vulnerable person's welfare.

8.2 Often a telephone, telephone number or other communications details may be the only information available to identify a person or to identify their next of kin or a person responsible for their welfare.

8.3 Equally communications data can help establish the facts relevant to a person's death or serious injury, where no crime has occurred.

8.4 Under the Act communications data may also be obtained and disclosed in serious welfare cases where it is necessary within the meaning of section 58(7)(g) and the conduct authorised or required is proportionate to what is sought to be achieved by obtaining the data.

Public Emergency Call Service (999/112 calls)

8.5 The Act regulates the acquisition and disclosure of communications data for the statutory purposes in section 58(7). The Communications Act 2003 also requires certain CSPs to provide communications data to the emergency services following an emergency call made to 999 and 112 emergency numbers.

8.6 To assist the emergency services and emergency operator further details in relation to handling 999 and 112 calls are contained within the Public Emergency Communications Service Code of Practice.

8.7 This code is not intended to regulate the handling of an emergency call but to ensure the boundary between this code and the Public Emergency Communications Services Code of Practice is clear. In so doing this code recognises an emergency period of one hour after the termination of the emergency call in which disclosure of communications data to emergency services will largely fall outside the provisions of the Act.

8.8 CSPs must ensure that any service user can access the emergency authorities by using the emergency numbers and, to the extent technically feasible, make caller location information available to the emergency authorities for all 999/112 calls. In practice this means sufficient detail to identify the origin of the emergency call and, if appropriate, to enable the deployment of an emergency service to the scene of an emergency.

8.9 It is usual for CSPs to disclose, at the time of the call, some identity (caller line identity) and caller location information data (fixed or mobile) to the emergency services in order to facilitate a rapid response to the emergency call.

8.10 CSPs should take steps to assure themselves of the accuracy of the information they may be called upon to disclose. Any known limitations in this accuracy, particularly for location, should be proactively disclosed to the emergency services.

8.11 The emergency service can call upon an emergency operator or relevant service provider to disclose data about the maker of an emergency call within the emergency period within one hour of the 999/112 call.

8.12 It is appropriate for the emergency service or emergency operator to require the CSP to disclose any further caller location information that might indicate the location of the caller at the time of the emergency call. Within one hour of the 999/112 call, it is also appropriate for the CSP, acting in the belief that information might assist the emergency service to respond effectively or efficiently to the emergency, to proactively disclose to the emergency service or emergency operator any further caller location information (CLI) about the location of the caller at the time of the emergency call.

8.13 If an emergency call is disconnected prematurely for any reason, technical or otherwise, and the emergency operator is aware or is made aware of this, then the emergency operator can elect to represent the data disclosed when the call was put to the emergency service initially. This voluntary disclosure would fall outside the scope of the Act.

8.14 Some CSPs have provided secure auditable communications data acquisition systems for the disclosure of communication data under the Act. Where these exist, it is appropriate for emergency services to be provided with accreditation details to use them for acquiring data about the maker of an emergency call or caller location information, as appropriate, during the emergency period.

8.15 When a secure auditable system is not available, a manual application for data can be made. The Public Emergency Communications Service Code of Practice contains the process to be followed[48].

8.16 If the emergency call is clearly a hoax, there is no emergency. Where an emergency service concludes that an emergency call is a hoax and the reason for acquiring data in relation to that call is to detect the crime of making a hoax call – and not to provide an emergency service – then the application process under the Act must be undertaken.

8.17 Should an emergency service require communications data relating to the making of any emergency call after the expiry of the emergency period of one hour from the termination of the call, that data must be acquired or obtained under the provisions of the Act.

8.18 Where communications data about a third party (other than the maker of an emergency call) is required to deal effectively with an emergency call, the emergency service may make an urgent oral application for the data. Disclosure of that data would also fall within under the provisions of the Act.

8.19 Increasingly, members of the public are using non-emergency numbers to request assistance.

8.20 A caller might dial either 101 or 111 to seek non-emergency assistance (or Crimestoppers on 0800 555 111 should they wish to report crime anonymously). In the case of calls to 101, 111 and other relevant non-emergency assistance services, the call handler might believe it is more appropriate that an emergency response is made[49]. If insufficient details are available to provide an emergency response it is appropriate for the call handler to seek assistance using the 999/112 numbers if that act would speed up the provision of emergency assistance. If necessary, it is also appropriate for the call handler to contact a CSP to seek sufficient subscriber or other communications data, as are necessary and appropriate to assist with the provision of an emergency response.

8.21 The Act does not seek to regulate either the actions of the call handler or the provision of data by the CSP.

---

[48] To be used with the Public Emergency Communications Service Code of Practice, there is a guide specifically for emergency operators and emergency authority control room staff on when it is appropriate to contact CSPs.

[49] Guidance regarding non-emergency numbers is available from the KET (ketadmin@college.pnn.police.uk). It sets out what records need to be retained so that audit and oversight activities can take place. This emergency process is not to be used in support of activity to investigate hoax or malicious callers or for other situations where the call handler does not have a belief that an emergency situation has arisen. Where a call starts as a non-emergency but develops into an emergency call then paragraphs 8.12 would apply.

Malicious and nuisance communications

8.22 Many CSPs offer services to their customers to deal with complaints concerning malicious and nuisance communications. Although these services vary, all CSPs believe that such calls can be very distressing for their customers and that every effort should be made to resolve such situations as efficiently and effectively as possible.

8.23 The victim of malicious or nuisance communications may, in the first instance, bring it to the attention of their CSP or report it to the police.

8.24 When contacted directly by a customer, the CSP may consider the circumstances of the complaint are such that the customer should be advised to report the matter without delay to the police for investigation.

8.25 Additionally the CSP can offer practical advice on how to deal with nuisance communications and may, for example, arrange a change of telephone number. The advice given by the CSP may indicate that the circumstances could constitute a criminal offence. The CSP may choose to disclose data to its customer relating to the source of the malicious or nuisance communications, but must ensure that the disclosure complies with the provisions of both the DPA and the Privacy and Electronic Communications Regulations (2003).

8.26 Upon receipt of a complaint a CSP may retrieve and retain relevant specific data that, if appropriate, can be disclosed to the police later. If the complainant wishes the matter to be investigated, it is essential for the CSP and the police[50] to liaise with one another to ensure the lawful disclosure of data to enable any offence to be effectively investigated.

8.27 Where the complainant reports a matter to the police that has been previously raised with the CSP, any data already collated by the CSP may be disclosed to the police SPoC under the provisions of the DPA or the Privacy Regulations[51]. Subsequent police investigation may require the acquisition or disclosure of additional communications data from the complainant's CSP or other CSPs under the provisions of the Act.

8.28 Whether the initial complaint is reported to the CSP or directly to the police, careful consideration should be given to whether the occurrence of malicious or nuisance communications are, or may be, related to other incidents or events. Specifically, this could be where the complainant is a victim of another crime or is a witness or a member of a trial jury in ongoing or forthcoming criminal proceedings.

[50] Ordinarily this will be overseen and coordinated by the police force's SPoC.

[51] Regulation 15 concerns tracing of malicious or nuisance calls.

9 The request filter

9.1 The request filter will provide an additional safeguard on the acquisition of communications data. It will work alongside other acquisition safeguards and existing infrastructure to limit the volume of communications data being provided to a public authority.

9.2 Only specified communications data defined in an authorisation will be processed by the request filter. The specified data must be necessary and proportionate for the operational requirement set out in the authorisation and can only operate on limited sets of authorised data using specified processing patterns. The request filter will only retain communications data temporarily whilst the data is being processed. Once processing is complete the data will be deleted.

9.3 The request filter is available to all public authorities to assist in obtaining the communications data that they are permitted to use, subject to individual authorisations. It will support complex communications data investigations where multiple sets of data need to be correlated. The filter will assist public authorities by:

- Providing a mechanism for pulling fragmented communications data together and providing a more complete analysis. With the increasing use of a wider range of online communications services and communications networks, the communications data required to answer operational questions is becoming more fragmented;

- Reducing analytic burden on public authorities and getting an operational answer in the shortest possible time to facilitate the timely recovery of forensic evidence, eliminate individuals without further more intrusive activity, and identify witnesses while events remain fresh in their memories; and

- Managing proportionality and collateral intrusion. A public authority will only be provided with the data that directly answers its question, as opposed to all the data originally required to conduct the analysis.

9.4 The request filter will be available to all public authorities. The SIA can acquire data in bulk under the provisions in part 6 of the Act and select that data for examination for operational purposes specified in the warrant. In considering whether a bulk warrant is necessary and proportionate, the Secretary of State and Judicial Commissioner must take into account whether the information it is considered necessary to obtain under the warrant could reasonably be obtained by other means. This consideration should include whether the required information could reasonably be obtained through a less intrusive power such as the targeted acquisition of communications data or the targeted acquisition of communications data using the request filter.

Authorisations

9.5 The request filter can be used to obtain and process data as part of a targeted communications data authorisation.

9.6 During the development of an application, the SPoC may advise applicants of situations where it would be appropriate to make use of the request filter and its capabilities in order to manage collateral intrusion.

9.7 The request filter may be identified as part of the approach to managing collateral intrusion in an authorisation. The request filter will only disclose records that match specified criteria to the SPoC and applicant. In making such a case, the authorisation should consider the likely effectiveness of the specified criteria in achieving the expected reduction in records. For example if the question to the request filter is 'who was in location A at time N and location B at time M', effectiveness will depend on, for example, the distance between the locations and any links between the locations such as main roads and railway lines.

9.8 The designated senior officer, with advice from the SPoC, and taking account of information provided by the request filter on the volumes of data that may be disclosed, should consider the proportionality of:

- The data to be disclosed to the request filter by the CSPs; and
- The data to be disclosed to the applicant by the request filter.

9.9 Consideration of proportionality for authorisations involving the request filter should take into account future evidential requirements. Particular consideration should be given as to whether it will be possible to evidence any records disclosed by the request filter through secondary communications data authorisations or other means. For example, if the question to the request filter is 'who was in location A at time N and location B at time M', it may be possible to evidence that any individuals identified were indeed in the specified locations through a secondary communications data authorisation seeking the locations of those identified individuals at times N and M.

9.10 The authorisation should also consider the proportionality of the data to be disclosed to the request filter by the CSPs, even if the majority is not expected to be released to the public authority.

9.11 As with other authorisations, the designated senior officer may place constraints on the release of any results from the filter so that if the number of results is greater than expected, disclosure to the public authority will be prevented.

Making use of the request filter

9.12 The SPoC is responsible for monitoring the request filter progress and managing compliance with the relevant authorisation.

9.13 The request is sent to the filter which in turn identifies the relevant communication service providers for the request and requires them to disclose the authorised communications data only to the request filter. They will not be aware of the detail of the processing to be undertaken.

9.14 Depending on the nature of the communications data and processing, the request filter may require decisions to be made by the SPoC during the processing. For example if there is a delay with one of the data sources it may be desirable for operational purposes to make use of intermediate results once a certain amount of data has been received. In this situation, the authorised processing must be allowed to complete so that the full set of results is obtained. Where there is any doubt regarding the compliance with an authorisation of activity to be undertaken by the request filter, the SPoC may be approached for confirmation.

9.15 The request filter performs the authorised processing of the communications data that has been disclosed to produce a results file. The only communications data that is processed is that disclosed by the communications providers for the purpose of the relevant authorisation. Only the results from the filter processing are released to the SPoC. An additional check may be used prior to release to confirm that the number of results are within specified limits.

Data management

9.16 The request filter will be operated on behalf of the Secretary of State by the Home Office. In practice the service will be provided by one or more third parties under contract.

9.17 The data owner for any authorised communications data disclosed to the request filter will be the designated senior officer at the authorising public authority. The data processor for all data disclosed to the request filter will be the Home Office (or another public authority designated by the Secretary of State by regulations). Once any data is disclosed to a public authority, that public authority is the data owner and processor for that disclosed data.

9.18 The communications data associated with an authorisation will be temporarily retained in the request filter until either the authorised processing is complete or, prior to that it ceases to be necessary to retain the data for the purpose concerned.

9.19 Those operating the request filter may periodically check with the relevant SPoC whether an authorisation remains valid if it has not been able to complete the processing. In any case, the relevant SPoC should notify the request filter immediately if the purpose of an authorisation is no longer valid so that any communications data associated with that authorisation is deleted and any outstanding or further data requests are cancelled.

9.20 Once the results have been released and the authorisation is complete, the disclosed communications data (including the results) are deleted from the request filter. Only audit and logging data is retained in the filter in accordance with requirements in the Act. This deletion is independent of CSP retention systems which will continue to hold the data for their normal retention period.

9.21 The request filter will only disclose communications data to the person identified in the relevant authorisation, or the designated senior officer concerned in accordance with section 66 of the Act.

9.22 The Secretary of State may in addition permit designated individuals to read, obtain or otherwise process data for the purposes of support, maintenance, oversight, operation or administration of the request filter.

9.23 The request filter will generate management and reporting information for a number of purposes including:

- Providing designated senior officers with information to inform decisions on the necessity and proportionality of authorisations;
- Support, maintenance, oversight, operation or administration of the arrangements; and
- The functions of the Investigatory Powers Commissioner.

9.24 This information may only be disclosed to:

- Designated senior officers for the purposes of determining the necessity and proportionality of an authorisation;
- Individuals designated by the Secretary of State for the purposes of support, maintenance, oversight, operation or administration of the request filter;
- The Investigatory Powers Commissioner for the purposes of the functions of the Commissioner; or
- When otherwise authorised by law.

9.25 Given the sensitivity of the data handled by the request filter, the Secretary of State must ensure that sufficient protections are in place to ensure the security of the system and protect against unauthorised and/or unlawful data retention, processing, access or disclosure. The filter will be operated under government security accreditation in accordance with government security policies and relevant standards. This will cover as a minimum:

- Protection of personal data disclosed by CSPs to the request filter in accordance with an authorisation;
- Controls, monitoring and audit of access to and use of the request filter;
- Restrictions regarding disclosure of results from the request filter;
- Provisions for deletion of material when no longer necessary or proportionate to retain it; and
- Those provisions outlined in chapter 11 regarding data protection.

9.26 Data disclosed to the public authority as a result of use of the request filter must be handled in accordance with the detail outlined in chapter 11.

Oversight and reporting

9.27 The request filter will be overseen by the Investigatory Powers Commissioner who will keep the use of the request filter by public authorities under review. This will form part of the Commissioner's broader audit, inspection and investigation regime for public authorities and their acquisition of communications data.

9.28 The Secretary of State must consult the Investigatory Powers Commissioner about the principles on the basis of which the request filter will be established, maintained or operated.

9.29 The Investigatory Powers Commissioner will receive an annual report regarding the functioning of the request filter during that year. The report will include details of verification and quality assurance activities, data deletion, security arrangements, and the operation and use of the arrangements. The Commissioner may use the information to inform its audit and inspection activities, and may conduct investigations into any specific issues arising from the report. As a result the Commissioner may require changes to be made to the use, operation, or design of the filtering arrangements.

9.30 The error reporting provisions detailed in Chapter 21 apply to the request filter. Should any significant processing errors occur which give rise to a contravention of any requirements in Part 3 of the Investigatory Powers Act, the fact must be reported to the Investigatory Powers Commissioner immediately. Where one technical system error occurs it could have multiple consequences. Such errors could, for example include the omission of, or incorrect matches in filtered results, or the release of results that exceed specified thresholds. For more detail see Chapter 21.

10 Maintenance of a technical capability

10.1 CSPs may be required under section 229 of the Act to provide a technical capability to give effect to a notice or authorisation under Part 3. The purpose of maintaining a technical capability is to ensure that, when a Part 3 notice or authorisation is in place, companies can give effect to it securely and quickly. In practice, these requirements will only be placed on companies that are required to give effect to notices or authorisations on a recurrent basis.

10.2 The Secretary of State may give a relevant CSP a "technical capability notice" imposing on the relevant operator obligations specified in the notice, and requiring the person to take all steps specified in the notice.

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

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

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

10.5 In the event that a number of CSPs are involved in the provision of a service, the obligation to provide a capability, and to remove encryption, will be placed on the CSP which has the technical capability to give effect to the notice and on whom it is reasonable practicable to impose these requirements.

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

Consultation with service providers

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

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

Matters to be considered by the Secretary of State

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

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

- The likely benefits of the notice – this may take into account projected as well as existing benefits;
- The likely number of users (if known) of any postal or telecommunications service to which the notice relates – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the technical capability notice;
- The technical feasibility of complying with the notice – taking into account any representations made by the communications service provider and giving specific consideration to any obligations in the notice to remove electronic protections (as described at section 231(4));
- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the company as part of the notice, such as those relating to security. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money; and
- Any other effect of the notice on the communications service provider – again taking into account any representations made by the company.

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

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

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

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

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

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

Giving a technical capability notice

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

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

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

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

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

10.17 A person to whom a technical capability notice is given is under a duty to comply with the notice. The duty to comply with a technical capability notice to give effect to communications data authorisations is enforceable against a person in the UK and a person outside the UK by civil proceedings by the Secretary of State.

Disclosure of technical capability notices

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

10.19 Any person to whom a technical capability notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence or contents of that notice to any person[52].

10.20 Section 231(8) provides for the CSP to disclose the existence and contents of a data retention notice with the permission of the Secretary of State. Such circumstances are likely to include disclosure:

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

Regular review

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

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

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

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

[52] See section 231(8)

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

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

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

Variation of technical capability notices

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

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

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

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

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

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

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

10.33 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraphs 10.9-10.12.

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

Revocation of technical capability notices

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

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

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

11 General safeguards

11.1 This section relates to data protection requirements for data held by a public authority which was acquired under Part 3 of the Act.

11.2 Communications data acquired or obtained under the provisions of the Act may only be held for one or more of the statutory purposes for which the public authority can acquire communications data. Any data obtained through the Act, and all copies, extracts and summaries of it, must be handled and stored securely in accordance with the relative sensitivity of the data. Such data as is held should be adequate, relevant and not excessive in relation to the purpose.

11.3 In addition, the requirements of the DPA[53] and its data protection principles must be adhered to.

11.4 Communications data held by a public authority should be treated as information with a classification of OFFICIAL and a caveat of SENSITIVE, though it may be classified higher if appropriate[54]. The SENSITIVE caveat is for OFFICIAL information that is subject to 'need to know' controls so that only authorised personnel can have access to the material. This does not preclude, for example, the disclosure of material or the use of this material as evidence in open court when required. Rather, the classification and caveat of OFFICIAL - SENSITIVE makes clear that communications data must be treated with care, noting the impact on the rights to privacy and, where appropriate, freedom of expression of the subjects of interest and, depending on the data, possibly some of their communications contacts.

11.5 Communications data that is obtained directly as a consequence of the execution of an interception warrant must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 51 of the Act.

11.6 Communications data acquired under the Act must be held in a manner which provides the adequate level of protection for the relative sensitivity of the data and meets the data protection principles outlined in the DPA. Data must be effectively protected against unauthorised access to and use of that data, with particular consideration given to the principles of data security and integrity.

11.7 Access to communications data must be limited to the minimum number of trained individuals necessary for the authorised purposes. Individuals should be granted access only where it is required to carry out their function in relation to one of the purposes for which the public authority may acquire communications data.

---

[53] Guidance is available from www.justice.gov.uk/information-access-rights/data-protection *or* www.ico.org.uk.

[54] Details of government security classifications can be found at https://www.gov.uk/government/publications /government-security-classifications. Those who do not use these classifications should treat information in the appropriately equivalent manner under their data security rules.

11.8 A public authority may disclose communications data acquired under the Act only to the minimum extent necessary. The individual or organisation to which it is to be disclosed must require access for purposes consistent with those in the Act. On occasions where it is necessary for a public authority to disclose data to an overseas authority, the process outlined in paragraphs 11.29 – 11.33 should be followed.

11.9 When sharing data, the relevant public authority must be satisfied that the data will be adequately protected and that safeguards are in place to ensure this. All data shared must be afforded the same protections as it would receive at the public authority which originally acquired it. Appropriate limitations must be placed on the number of people to whom material is disclosed and the extent to which material is disclosed.

11.10 Data may only be held for as long as the relevant public authority is satisfied that it is still necessary for a statutory purpose. When it is no longer necessary or proportionate to hold such data, all relevant data must be destroyed. Data must be deleted such that it is impossible to access at the end of the period for which it is required.

11.11 Where it is necessary to process communications data acquired under the Act, public authorities must ensure that this is carried out in accordance with the DPA principles. This includes only processing such data where it is necessary, lawful and with appropriate safeguards. Public authorities must ensure that appropriate measures are in place to prevent unauthorised or unlawful processing and accidental loss or destruction of, or damage to, this data.

11.12 Where it is necessary to process communications data acquired under the Act together with data from other sources, the public authority must ensure that either it remains possible to identify the source of the data and apply security provisions accordingly or the resultant combined data is subject to the same or more stringent security provisions.

Disclosure of communications data and subject access rights

11.13 This section of the code provides guidance on the relationship between disclosure of communications data under the Act, CSPs' obligations to comply with a notice to disclose data, and individuals' right of access under section 7 of the DPA to personal data held about them.

11.14 The provisions regarding subject access requests[55] made under section 7 of the DPA apply notwithstanding the offence at section 79of the Act. However a CSP may rely on certain exemptions to the right of subject access under Part IV of the DPA[56].

[55] The Information Commissioner has produced a Subject Access Code of Practice to assist organisations adopt good practice when handling subject access requests, which is available at: ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf.

[56] There may be other bars to disclosure in other legislation, for example regarding impeding an investigation.

11.15 Section 28[57] of the DPA provides that data are always exempt from section 7 where such an exemption is required for the purposes of safeguarding national security.

11.16 Section 29 of the DPA provides that personal data processed for the purposes of the prevention and detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature are exempt from section 7 to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters.

11.17 The exemption to subject access rights possible under section 29 of the DPA does not automatically apply. In the event that a CSP receives a subject access request where the fact of a disclosure under the Act might itself be disclosed, the CSP concerned must carefully consider whether in the particular case disclosure of the fact of the authorisation would be likely to prejudice the prevention or detection of crime.

11.18 Where a CSP is uncertain whether disclosure of the fact of a notice would be likely to prejudice an investigation or operation, it should approach the SPoC of the public authority which gave the notice – and do so in good time to respond to the subject access request. The SPoC can make enquiries within the public authority to determine whether disclosure of the fact of the notice would likely be prejudicial to the matters in section 29. As paragraph 4.71 requires a notice to set out whether a CSP may inform the subject a request for their data has been made, such circumstances would be limited[58].

11.19 Where a CSP withholds a piece of information in reliance on the exemption in section 28 or 29 of the DPA, it is not obliged to inform an individual that any information has been withheld. It can simply leave out that piece of information and make no reference to it when responding to the individual who has made the subject access request.

11.20 A CSP should not provide information in response to a subject access request where doing so would be an offence under section 79 of the Act.

11.21 CSPs should keep a record of the steps they have taken in determining whether disclosure of the fact of a notice would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police. Under section 42 of the DPA an individual may request that the Information Commissioner assesses whether a subject access request has been handled in compliance with the DPA.

---

[57] Section 28(2) of the DPA makes clear that a certificate from a Minister of the Crown is conclusive evidence, though this can be challenged through appeal to a Tribunal.

[58] The SPoC must provide a response which will enable the CSP to comply with its obligations to respond to the subject access request within 40 days at the latest.

Acquisition of communication data on behalf of overseas authorities

11.22 While the majority of public authorities which obtain communications data under the Act have no need to disclose that data to any authority outside the United Kingdom, there can be occasions when it is necessary, appropriate and lawful to do so in matters of international co-operation.

11.23 There are two methods by which communications data, whether obtained under the Act or not, can be acquired and disclosed to overseas public authorities[59]:

- Judicial co-operation; or
- Non-judicial co-operation.

Neither method compels United Kingdom public authorities to disclose data to overseas authorities. Data can only be disclosed when a United Kingdom public authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled.

Judicial co-operation

11.24 A central authority in the United Kingdom may receive a request for mutual legal assistance (MLA) which includes an application for communications data from an overseas court exercising criminal jurisdiction, an overseas prosecuting authority, or any other overseas authority that appears to have a function of making requests for MLA. This MLA request must be made in connection with criminal proceedings or a criminal investigation being carried on outside the United Kingdom, and the application for communications data included must be capable of satisfying the requirements of Part 3 of the Act.

11.25 If such an MLA request is accepted by the central authority, it will be referred for consideration by the appropriate public authority in the UK. The application may then be considered and, if appropriate, executed by that public authority under section 58 of the Act and in line with the guidance in this code of practice.

11.26 In order for a notice or authorisation to be granted, the United Kingdom public authority must be satisfied that the application meets the same criteria of necessity and proportionality as required for a domestic application.

Non-judicial co-operation

11.27 Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries. These can include applications for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such an application, the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Part 3 of the Act.

11.28 The United Kingdom public authority must be satisfied that the application complies with United Kingdom obligations under human rights legislation. The necessity and proportionality of each case must be considered before the authority processes the authorisation or notice.

---

[59] This includes public authorities within the Crown Dependencies and the British Overseas Territories.

Disclosure of communications data to overseas authorities

11.29 Where a United Kingdom public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring the data to that authority, it must consider whether the data will be adequately protected outside the United Kingdom and what safeguards may be needed to ensure that. Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

11.30 If the proposed transfer of data is to an authority within the European Union, that authority will be bound by European data protection legislation and its national data protection legislation. Any data disclosed will be protected there without need for additional safeguards.

11.31 If the proposed transfer is to an authority outside of the European Union and the European Economic Area (Iceland, Liechtenstein and Norway), then it must not be disclosed unless the overseas authority can ensure an adequate level of data protection. The European Commission has determined that certain countries, for example Switzerland, have laws providing an adequate level of protection where data can be transferred without need for further safeguards[60].

11.32 In all other circumstances, the United Kingdom public authority must decide in each case, before transferring any data overseas, whether the data will be adequately protected there. The Information Commissioner has published guidance on sending personal data outside the European Economic Area in compliance with the Eighth Data Protection Principle, and, if necessary, his office can provide guidance.

11.33 The DPA recognises that it will not always be possible to ensure adequate data protection in countries outside of the European Union and the European Economic Area, and there are exemptions to the principle, for example if the transfer of data is necessary for reasons of 'substantial public interest'[61]. There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data. That is a decision that can only be taken by the public authority holding the data on a case by case basis.

[60] The relevant Commission webpage is at: http://ec.europa.eu/justice/data-protection//international-transfers/adequacy/index_en.htm.

[61] Paragraph 4, Schedule 4, DPA.

12 Compliance and offences

12.1 The Act places a requirement on CSPs to comply with a requirement imposed on them by a notice under Part 3 of the Act, but are not required to take any steps which it is not reasonably practicable for them to take. Where a technical capability notice is in place an operator will be considered as having put in place the capabilities specified in that notice when consideration is given to their compliance with a notice.

12.2 What is reasonably practicable will be considered on a case-by-case basis, taking into account the individual circumstances of the relevant CSP. Such consideration is likely to cover a number of factors including, but not limited to, the technical feasibility and likely cost of complying with the notice.

12.3 Where a technical capability notice is in place an operator will be considered as having put in place the capabilities specified in that notice when consideration is given to their compliance with the obligation.

12.4 Section 82 of the Act provides that where such a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given in any of the following ways:

- By serving it at the person's principal office within the UK or, if the person does not have an office in the UK, at any place in the UK where the person carries on business or conducts activities;
- At an address in the UK specified by the person;
- By notifying the person by such other means as the authorised officer considers appropriate (which may include notifying the person orally).

12.5 When considering whether a notice given to a person outside the UK is reasonably practicable, section 82(4)(a) specifies that regard must be had to any requirements or restrictions under the law of the country where the CSP is based that are relevant to the taking of those steps. It also makes clear the expectation that CSPs will seek to find ways to comply without giving rise to conflict of laws. What is reasonably practicable should be agreed after consultation between the CSP and the Government. If no agreement can be reached it will be for the Secretary of State to decide whether to proceed with civil proceedings.

12.6 The duty of compliance in relation to Part 3 of the Act is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988 or for any other statutory relief.

Offences

12.7 The Act creates two offences which are relevant to the acquisition and disclosure of communications data.

Acquisition Offence

12.8 Under section 11 of the Act, it is an offence for a person in a public authority knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority.

12.9 The creation of the offence of unlawfully obtaining communications data reflects the sensitivity of communications data and the need for careful consideration in authorisation of its acquisition. The roles and responsibilities laid down for the senior responsible officer, designated senior officer and SPoC are designed to prevent the 'knowing or reckless' acquisition of communications by a public authority where it does not hold a lawful authorisation. Proper adherence to the requirements of the Act and this code, including following the procedures identified in chapter 4, will ensure no offence is committed.

12.10 It is a defence if the person who obtained the communications data can show that action was taken in the reasonable belief that they had, in law, the right to obtain that data.

12.11 This offence is not designed to capture errors on behalf of the public authority but rather, for example, instances where a person in a public authority failed to take account of obvious risk or where a person in a public authority deliberately fails to obtain an authorisation or obtains communications data from a CSP despite the fact that they could not have genuinely believed that an authorisation would be in place.

12.12 In particular, it is not an offence to obtain communications data where it is made publicly or commercially available by the CSP or otherwise where the CSP freely consents to its disclosure. In such circumstances the consent of the operator provides the lawful authority for the obtaining of the data.

Disclosure offence

12.13 Under section 79, it is an offence for a telecommunications operator to disclose without reasonable excuse the existence of a request for communications data by a public authority under the Act.

12.14 The offence of unauthorised disclosure occurs when any CSP, or employee of a CSP, reveals the existence of either a requirement to disclose communications data about a particular person to that person.

12.15 It is a reasonable defence for a CSP to disclose such information when the public authority making the request for data gives permission to do so. A public authority must indicate in the authorisation for obtaining of communications data whether it gives permission to the CSP to disclose the request for communications data. If permission is given, the public authority must specify to the CSP the circumstances under which disclosure may take place.

12.16 When considering whether or not to give permission to disclose the existence of a specific request for communications data, the public authority must consider the specific circumstances of the operation or investigation to which the request refers. Where no circumstances preventing disclosure are identified, permission should be given.

12.17 Circumstances which may prevent permission being given may include, but are not limited to:

- The interests of other public authorities in the operation or investigation;
- Any potential negative impact on future operational or investigative capability; and
- The undermining of the purposes outlined in section 58(7) of the Act.

12.18 Circumstances in which it may be appropriate to give permission to disclose the existence of a specific request for communications data may include where communications data is requested to assist in the investigation of a crime of which the subject of the request is the victim – for example where a person's phone has been stolen and the police seek communications data in order to locate the phone.

12.19 It would not be a reasonable defence for a CSP to disclose such information in the interests of transparency to its customers without the permission of the relevant public authority.

Part 3

Communications Data Retention

13 General extent of powers

Necessity and proportionality

13.1 Section 84(1) of the Act gives the Secretary of State the power to issue a data retention notice to a CSP, requiring them to retain relevant communications data, if it is considered necessary and proportionate for data to be retained for one or more of the purposes in section 58(7) of the Act. These are:

- In the interests of national security;
- For the purpose of preventing or detecting crime[62] or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- In the interests of public safety;
- For the purpose of protecting public health;
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- For the purpose, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- To assist investigations into alleged miscarriages of justice;
- For the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime (such as a natural disaster or an accident);
- In relation to a person who has died or is unable to identify himself, for the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for his death or condition; and
- For the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.

13.2 Section 2 of the Act requires the Secretary of State to have regard to the following when giving, varying or revoking a notice:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means,
- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.

---

62 Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed. See section 239(1) of the Act.

13.3 Data retained for the purposes set out above can only be accessed by public authorities for those purposes under Part 3 of the Act, or other appropriate statutory regime, where it is necessary and proportionate to do so. The consideration of necessity and proportionality involves balancing the extent of the interference with an individual's right to respect for their private life and, where relevant, with freedom of expression, against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest. Further information on this can be found in chapter 3 of this code.

14 Giving of data retention notices

Process for giving a data retention notice

14.1 The Home Office and key operational agencies (including law enforcement agencies and security and intelligence agencies) maintain governance arrangements in order to identify operational requirements, including the potential requirement to issue a data retention notice.

14.2 Once a potential requirement is identified, the Home Office will consult the relevant CSP(s) and, if appropriate, the Secretary of State will consider giving a notice.

Criteria for issuing a data retention notice

14.3 When considering whether to issue a notice a number of factors are taken into account. These include, but are not limited, to:

- The size of a CSP – a CSP with a larger customer base is more likely to receive a data retention notice;
- The speed of growth of a CSP – small CSPs with rapid prospective growth may receive notices in anticipation of future law enforcement requirements;
- The number of requests a CSP receives annually for communications data – this, and the CSPs ability to meet the volume of requests they receive, will be a key determinant of whether there is benefit in serving a notice on a CSP (noting that the giving of a notice may increase the number of requests received by a CSP);
- Whether a CSP operates a niche service – a CSP which is the sole or key provider of a type of service may receive a notice regardless of the size of the company; or
- Whether a CSP operates in a specific geographical area – a CSP which is a key provider of services in a limited geographical area is more likely to receive a notice.

14.4 Ultimately, however, a notice can only be given where the Secretary of State, having taken into account relevant information, considers it necessary and proportionate to do so.

14.5 The timescale for such processes will depend on operational need but will always follow the same steps to ensure that the Secretary of State is making an informed decision, based on the relevant information.

14.6 Where a company uses the physical network (this includes the network bandwidth and phone lines) belonging to another in order to provide their services to the public, a retention notice can be imposed on whichever company holds the relevant communications data (which will depend on how they design and operate their systems). The Home Office will work with providers to ensure that public authorities are aware of which company is best placed to respond to requests for the data.

14.7 Where two companies under a retention notice hold similar or identical data or are capable of doing so the Home Office will agree an approach with the providers concerned to ensure that the relevant data is not retained more than once.

Criteria for giving a notice to categories of providers

14.8 There may be circumstances where there are a number of CSPs providing similar services in a specific limited area. An example of this could be Wi-Fi providers in a particular location.

14.9 It is possible that the Secretary of State could place the same obligations on all such CSPs through one notice, but only if it was considered necessary and proportionate to do so.

14.10 While this may be appropriate for a relatively small number of providers providing the same or a similar service, this provision cannot be used to place blanket requirements across a large number of companies operating a service or companies providing a range of different services, not least because the requirements in a notice need to reflect the particular nature of each business.

Consultation with service providers

14.11 Before giving a notice to a company the Secretary of State must take reasonable steps to consult any CSP(s) which will be subject to the notice.

14.12 In practice, consultation is likely to take place long before giving a notice to a company. The Home Office will engage with companies who may possibly be subject to a notice in the future to provide advice and guidance and prepare them for the possibility of receiving a notice should it be considered necessary and proportionate to do so.

14.13 Should the giving of a notice to a CSP be deemed appropriate, the Home Office will take steps formally to consult the company before giving a notice, in order to ensure that it accurately reflects the services and data types processed by that CSP and to ensure that the CSP understands the obligations being placed on it, including those in relation to the audit functions of the Information Commissioner.

14.14 Should a CSP have concerns about whether the requirements of a notice are appropriate or technically feasible, these should be raised during this consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process. Should a CSP continue to have concerns in respect of the feasibility of a notice once given they may refer the notice for review (see chapter 20).

14.15 Should it be considered appropriate to place the same obligations on a number of companies through one notice, the Home Office will take steps to consult all CSPs who would or could be affected by the notice. However, it is recognised that there may be cases where this will not be possible, for example where a new CSP enters the market after a notice is given and therefore will not have been formally consulted. In such circumstances the Secretary of State must take reasonable steps to consult any relevant CSP(s) which enter the market after such a notice is issued.

Matters to be considered by the Secretary of State

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

14.17 As part of the decision the Secretary of State must take into account a number of factors:

- The likely benefits of the notice – the extent to which the data to be retained may be of use to public authorities. This may take into account projected as well as existing benefits;
- The likely number of users of the services to be covered by the notice – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the data being retained;
- The technical feasibility of complying with the notice – taking into account any representations made by the CSP(s);
- The likely cost of complying with the notice – this will include the costs of both the retention, and any other requirements and restrictions placed on CSPs, such as ensuring the security of the retained data. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money[63]; and
- Any other impact of the notice on the CSP – again taking into account any representations made by the CSP(s).

14.18 The Secretary of State will also consider the contents of the proposed notice, including the data to be retained and the period or periods for which that data is to be retained up to a maximum of 12 months from the giving of the notice[64].

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

14.20 If the Secretary of State agrees with the recommendation to give a notice, they will then sign the notice.

Once a notice has been signed

14.21 Once a notice has been signed by the Secretary of State, arrangements will be made for this to be given to a CSP. During consultation with the CSP, it will be agreed who in the company should receive the notice and how it should be issued (i.e. electronically or in hard copy). If no recipient is agreed, then the notice will be issued to a senior executive within the company.

14.22 A data retention notice comes into force from the point it is given to the CSP, unless otherwise specified in the notice.

---

63 See paragraph 10.10 for details of the matters the Secretary of State will consider before issuing a data retention notice.

64 See paragraphs 14.30-14.37 for further information on retention periods.

14.23 It will often be the case that dedicated systems will be constructed within a CSP for the retention of communications data, and the time taken to design and construct such a system will be taken into account. Accordingly, different elements of the notice may take effect at different times.

14.24 Once a notice has been given to a CSP, a copy of the notice and any other relevant information will be sent to the Information Commissioner, who is responsible for auditing the security, integrity and destruction of retained data (see chapter 22 for further details).

The content of a data retention notice

14.25 A notice will set out:

- The CSP(s) to which it relates – where a company owns a number of subsidiary companies that operate under different trading names, the notice might additionally list these details for the sake of clarity;
- Which services data is to be retained for – it may not be necessary and proportionate to retain data in relation to all communication services provided by a company;
- The data to be retained and the period for which it is retained – these will relate to the categories of data listed as 'relevant communications data' in section 84(10) of the Act and will make clear whether certain categories of data should be retained for less than 12 months; and
- Any additional requirements or restrictions in relation to the retention of the data – this may include requirements in relation to the security, integrity and destruction of retained data and the audit of the CSPs compliance with these requirements by the Information Commissioner.

14.26 A notice will not necessarily represent the full range of services and data types which a CSP could retain. This does not mean that additional data types or services could not be included in a future version of the notice, should a pressing operational requirement arise, provided that it would be necessary and proportionate to do so (see chapter 15 for further details).

14.27 Requirements or restrictions in relation to the retention of the data may include:

- A requirement to take such steps as are necessary to ensure that data which is generated and processed by the CSP (including transitory information in the core systems) is made available to be retained; or
- A requirement to process the data to ensure that multiple items of data from a single or multiple CSP systems can be stored in a single clear record where appropriate to do so. This will ensure the volume of data retained is limited to that which is truly necessary.

Generation & processing of data

14.28 A retention notice may include requirements in relation to the retention of data. Such requirements may include:

- A requirement to retain data in such a way that it can be transmitted efficiently and effectively in response to requests (including linking events to user accounts);
- A requirement to take such steps as are necessary to ensure that data which is generated and processed by the CSP but not collected for business purposes is made available to be retained (this could include extracting or generating data from transitory information in the core network components or from network traffic);
- A requirement to process the data to ensure that multiple items of data from a single or multiple CSP systems can be stored in a single clear record where appropriate to do so; and
- A requirement to filter the data to remove records that are not of interest, including duplicate events or where aggregated records or summaries have been created;

14.29 Aggregation, summarisation and filtering of data will ensure the volume of data retained is limited to that which is truly necessary.

Retention period

14.30 Data retained under the Act may be retained for a maximum of 12 months.

14.31 A notice will only require data to be retained for as long as is considered necessary and proportionate, up to that maximum period. If, once a data retention notice is given, further evidence demonstrates that a retention period specified in the notice is no longer appropriate, the Secretary of State will set a different retention period, up to a maximum of 12 months, ensuring the period reflects what is necessary and proportionate.

14.32 A data retention notice may cover data already in existence at the point at which a notice is given or it may require the generation of data.

14.33 The starting point for the retention period for data in existence at the point of the notice is determined by the type of data.

14.34 The retention period for a specific communication commences on the day of the communication concerned. Some internet communications, such as broadband sessions, may remain active for days, or even months. In such cases the retention period commences on the day on which the communication ends.

14.35 For data held by a CSP about an entity to whom a service is provided the retention period commences on the day on which the entity concerned ceases to be connected to the service or if the data is changed. For example previous addresses for a customer may only be retained for 12 months after the CSP changes the data in their systems, irrespective of whether the customer remains with the service.

14.36 For all other communications data held by a CSP, including where data is required to be generated, then the retention period will start from the moment the data comes into existence.

14.37 Sometimes a CSP may already retain data for 12 months or more for business purposes. Such data may still be subject to a retention notice to ensure that the

data is available with the maximum 12 month period in case the business need for the data changes and the CSP decides to delete the data.

15 Review, variation and revocation of retention notices

Review

15.1 The Secretary of State must keep notices under review. This helps to ensure that a notice itself, or the retention of categories of data specified in a notice, remains necessary and proportionate.

15.2 It is recognised that, after a notice is given, a CSP is likely to require time to put the necessary capabilities in place to meet their obligations. As such, the first review should not take place until after these capabilities have been put in place. Without these capabilities being fully operational, it will not generally be possible to assess the benefits of a notice.

15.3 Reviews will take place at least once every two years once capabilities are in place. However, the exact timing of the review is at the Secretary of State's discretion.

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

- A significant change in demands by law enforcement agencies that calls into question the necessity and proportionality of the notice as a whole, or a subset of data being retained under a notice;
- A significant change in CSP activities or services; or
- A significant refresh or update of CSP systems.

15.5 The process for reviewing a notice is similar to the process for giving a notice, with the Home Office consulting operational agencies and CSPs as part of the review. In addition the Home Office will consult the Information Commissioner as part of the review.

15.6 The review will also take into account the number of law enforcement requests made and the age of the data obtained. An absence – or low volume – of law enforcement requests will not necessarily mean that it is no longer necessary and proportionate to maintain a data retention notice.

15.7 Once this process is complete, the Secretary of State will consider whether the notice remains necessary and proportionate.

15.8 A review may recommend the continuation, variation or revocation of a notice. Details of the variation of and revocation of data retention notices follow below.

15.9 The relevant CSP, the operational agencies and the Information Commissioner will be notified of the outcome of the review.

Variation

15.10 The communications market is constantly evolving and CSPs subject to data retention notices will often launch new services or generate new data that law enforcement may require.

15.11 CSPs subject to a data retention notice must notify the Home Office of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require data generated or processed in the course of providing those services to be retained.

15.12 Small changes, such as upgrades of systems or changes to data which are already covered by the existing notice, can be agreed between the Home Office and CSP in question. However, significant changes will require a variation of the data retention notice.

15.13 Section 89 of the Act provides that data retention notices can be varied by the Secretary of State. There are a number of reasons why a notice might be varied. These include:

- a CSP launching new services or generating new categories of communications data which may be of interest to law enforcement;
- changing law enforcement demands and priorities;
- a recommendation following a review (see review section above); or
- to amend or enhance the security requirements – for example following an audit of the security, integrity and destruction of retained data by the Information Commissioner.

15.14 Where a company has changed names, for example as part of a rebranding exercise or due to a change of ownership, the Home Office and the company will need to consider whether the existing notice is sufficient.

15.15 The process for varying a notice is similar to the process for giving a notice. The Home Office will consult operational agencies, to understand the operational impact of any change to the notice, and CSPs to understand the impact on them, including any technical implications. Once this consultation is complete, the Secretary of State will consider whether to vary the notice.

15.16 Further detail on the process for consultation with CSPs and consideration by the Secretary of State can be found in chapter 14.

15.17 Once a variation has been agreed by the Secretary of State, arrangements will be made for this to be given to a CSP. As with a data retention notice, a variation of a notice comes into force from the point it is given unless otherwise specified in the notice and different elements of the variation may take effect at different times.

15.18 Once a variation has been given to a CSP a copy will be sent to the Information Commissioner.

15.19 A data retention notice may be varied to reduce, or extend, the period for which data can be retained. No retention notice, or such variation, can result in data being retained for longer than 12 months.

Revocation

15.20 A data retention notice must be revoked (in whole or in part) if it is no longer necessary to require a CSP to retain communications data, or certain types of communications data.

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

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

15.23 Once notice of revocation has been given to a CSP a copy will be sent to the Information Commissioner.

16 Security, integrity and destruction of retained data

16.1 All data retained under the Act is subject to a range of safeguards in order to ensure effective protection of the data against the risk of abuse and any unlawful access to and use of that data. Section 87 of the Act requires CSPs under a notice to take steps to ensure that the data is adequately protected while it is being retained. These requirements relate to three broad areas – data security, data integrity and destruction of data.

16.2 Further detail on the security arrangements to be put in place by CSPs may be included in the data retention notice given to a CSP which, in accordance with section 84(7)(d), must specify any other requirements or restriction in relation to the retention of data.

16.3 In most cases data retained under a notice is stored in dedicated data retention and disclosure systems, which are securely separated by technical security measures (e.g. a firewall) from a CSPs business systems. Where data is retained by CSPs for business purposes for some, but not all, of the period specified in the notice, the data retention and disclosure system may hold a duplicate of that business data so that it can be accessed efficiently and effectively[65].

16.4 However, in some cases it will not be practical to create a duplicate of that data and CSPs will retain information in business or shared systems.

16.5 The scope of the security controls defined within this section apply to all dedicated IT systems that are used to retain or disclose communications data, and any other dedicated systems which are used to access, support or manage dedicated retention and disclosure systems. It also applies to all CSP (or third party) operational and support staff who have access to such systems. Additional security considerations may be required to enable systems for the disclosure of communications data to connect securely to acquisition systems in public authorities.

16.6 Where data is retained in business or shared systems, or where business systems are used to access, support or manage retention and disclosure systems, these will be subject to specific security controls and safeguards, similar to those defined within this section, where appropriate and as agreed with the Home Office.

65 In accordance with section 84(8)(a).

Data security

16.7 The specific data security measures required by a CSP to protect retained data will depend on a number of factors including, but not limited to, the volume of data being retained, the number of customers whose data is being retained and the nature of the retained data.

16.8 When setting security standards consideration must also be given to the threat to the data.

16.9 The security put in place at a CSP will comprise four key areas:

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

16.10 As each of these broad areas is complementary, the balance between these may vary e.g. a CSP with slightly lower personnel security is likely to have stricter technical and procedural controls. The specific security arrangements in place will be agreed in confidence between the Home Office and relevant CSPs and shared with the Information Commissioner for his functions under this code.

16.11 As the level of data security is based on a number of factors and is a balance of four broad areas, there is no single minimum security standard. However, all CSPs retaining data will be required to follow the key principles of data security set out in paragraphs 16.18 to 16.41. It is open to a CSP to put in place alternative controls or mitigations which provide assurance of the security of the data where agreed with the Home Office.

16.12 The Home Office will provide security advice and guidance to all CSPs who are retaining data and this will be provided to the Information Commissioner for the conduct of his functions under this code.

Data integrity

16.13 Data integrity, as required by section 86(1)(a), relates to a need to ensure that no inaccuracies are introduced to data when it is retained under the Act and that the data is not varied[66].

16.14 When relevant communications data is retained under the Act, it should be a faithful reproduction of the relevant business data and it should remain a faithful reproduction throughout any further processing that may occur during the period of its retention. A record of the business purpose for which the data is generated may be retained to assist law enforcement to understand the underlying quality and completeness of the business data which has then been retained. For example, data generated to assist a CSP in understanding network loading may be less accurate than data used to bill customers.

---

66 This includes at the point at which it is placed into a data retention and disclosure system and during the period of its retention.

16.15 There should be no errors introduced in retaining the data, for example in the process of copying the data to a retained data store or in searching and disclosing data, that lead to discrepancies between the business and retention sets of data.

16.16 Once the data has been retained, technical security controls shall be implemented to mitigate modification of the data, and to audit any attempt to modify the data, until such time that it is deleted in accordance with section 87(2) of the Act.

16.17 The audit capability of the data retention system shall be used to provide assurance that no unauthorised changes have been made to the retained data.

Principles of data security, integrity and destruction

Legal and regulatory compliance

16.18 All data retention systems and practices must be compliant with relevant legislation. As well as the Act, this includes, but is not limited to, the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003, which set out key controls in relation to the storage, use and transfer of personal data.

16.19 All systems and practices must also comply with any security policies and standards in place in relation to the retention of communications data. This may include any policies and standards issued by the Home Office, and any instruction or recommendation made by the Information Commissioner such as his published guidance on security. These further requirements are unlikely to be publicly available as they may contain specific details of security infrastructure or practices, disclosure of which could create additional security risks.

Information security policy & risk management

16.20 Each CSP must develop a security policy document. The policy document should describe the internal security organisation, the governance and authorisation processes, access controls, necessary training, the allocation of security responsibilities and policies relating to the integrity and destruction of data. Each CSP must also develop security operating procedures, including clear desk and screen policies for all systems. A CSP can determine whether this forms part of or is additional to wider company policies.

16.21 The security policy document and security operating procedures should be reviewed regularly to ensure they remain appropriate to the nature of the business, the data retained and the threats to data security.

16.22 Each CSP must identify, assess and treat all information security risks, including those which relate to arrangements with external parties.

Human Resources security

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

16.24 Staff with access to the data retention or disclosure systems should be subject to an appropriate level of security screening. The Government sponsors and manages security clearance for certain staff working within CSPs. CSPs must ensure that these staff have undergone relevant security training and have access to security awareness information.

Maintenance of physical security

16.25 Data retention and disclosure systems should have appropriate security controls in place. Access to the locations where the systems are both operated and hosted must be controlled such that access is limited to those with the relevant security clearance and permissions.

16.26 Equipment used to retain data must be sanitised and securely disposed of at the end of its life (see the section on destruction of data beginning at paragraph 16.42).

Operations management

16.27 Data retention and disclosure systems should be subject to a documented change management process, including changes to third party suppliers, to ensure that no changes are made to systems without assessing the impact on the security of retained data.

16.28 CSPs must also put in place a patching policy to ensure that regular patches and updates are applied to any data retention and disclosure system as appropriate. Such patches and updates will include anti-virus, operating systems, application and firmware. The patching policy, including the timescale in which patches must be applied, must be agreed with the Home Office.

16.29 CSPs should ensure that, where encryption is in place in data retention and disclosure systems, any encryption keys are subject to appropriate controls, in accordance with the security policy.

16.30 In order to maintain the integrity of internal data processing CSPs must ensure that data being processed is validated against agreed criteria.

16.31 Network infrastructure, services and system documentation must be secured and managed and an inventory of all assets should be maintained together with a clear identification of their value and ownership. All assets must be clearly labelled.

16.32 CSPs should also ensure that removable and storage media (including the hard drives used to store retained data) are managed in accordance with the security policy, especially when in transit.

16.33 The data retention and disclosure system, and its use, should be monitored and all audit logs compiled, secured and reviewed by the CSP security manager at appropriate intervals. These should be made available for inspection by the Home Office as required.

16.34 CSPs should ensure that systems are resilient to failure and data loss by creating regular back-ups of the data.

16.35 Technical vulnerabilities must be identified and assessed through an independent IT Health Check which must be conducted annually. The scope of the Health Check must be agreed with the Home Office.

Access controls

16.36 CSPs must ensure that registration and access rights, passwords and privileges for access to dedicated data retention and disclosure systems are managed in accordance with their security policy. They must also ensure that users understand and formally acknowledge their security responsibilities.

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

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

Management of incidents

16.39 CSPs must put in place clear incident management processes and procedures, including an escalation path to raise issues to senior management and the Home Office. Any breaches under relevant legislation, such as the Act or the Privacy and Electronic Communications Regulations 2003, should be notified in accordance with those provisions.

16.40 Measures should be implemented to prevent unauthorised disclosure or processing of data. Any suspected or actual unauthorised disclosure or processing of data or information must be reported as set out above.

16.41 System managers must ensure that data retention and disclosure systems enable the collection of evidence (e.g. audit records) to support investigation into any breach of security.

Additional requirements relating to the destruction of data

16.42 Section 87(2) makes clear that retained data must be destroyed[67] such that it is impossible to access at the end of the period for which it is required to be retained, unless its retention is otherwise authorised by law. A system must be set up such that it is verifiable that data is deleted and inaccessible at the end of the retention period. Deletions must take place at intervals no greater than monthly.

16.43 Where the physical, personnel and procedural security measures are assessed by the Home Office, or Information Commissioner, to be sufficient to prevent unauthorised physical access to the data retention and disclosure system, then data should be deleted in such a way that protects against data recovery using non-invasive attacks (i.e. attempts to retrieve data without additional assistance from physical equipment).

[67] Section 239(1) defines 'destroy' for the purposes of the Act to mean 'delete the data in such a way as to make access to the data impossible.'

16.44 Where the implemented security measures are assessed by the Home Office, or Information Commissioner, to be insufficient to protect the data retention and disclosure system against physical access by unauthorised personnel, then additional requirements for the secure destruction of retained data should be agreed with the Home Office and Information Commissioner on a case-by-case basis.

Additional requirements relating to the disposal of systems

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

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

16.47 If the equipment is to be finally disposed of, it must be securely sanitised by means of physical destruction by a Home Office approved supplier.

16.48 Sanitisation or destruction of data must include retained data copied for back-up and recovery, and anything else that stores duplicate data within the CSP system, unless retention of the data is otherwise authorised by law.

17 Disclosure and use of data

Disclosure of data

17.1 As per section 87 of the Act, a CSP must put in place adequate security systems (including technical and organisational measures) governing access to retained communications data in order to protect against any unlawful disclosure.

17.2 Section 84(8)(a) of the Act also requires CSPs to retain data in such a way that it can be transmitted efficiently and effectively in response to requests for communications data. The Home Office will work with CSPs to ensure that the necessary secure auditable systems are in place to enable this disclosure.

17.3 The provisions on disclosure of retained data are intended to cover disclosure of communications data in response to requests made under Part 3 of the Act. However, there may be other circumstances in which CSPs may lawfully disclose retained communications data. Such circumstances could include:

- If an emergency service requests data in relation to an emergency call (chapter 8);
- Requests for personal data held by a company via a subject access request under the Data Protection Act 1998[68];
- Where a CSP proactively discloses communications data to relevant public authorities or regulatory bodies such as in cases of suspected criminality.

Use of data by communications service providers

17.4 If data is held subject to a notice and would not otherwise be held by the CSP for business purposes, it should be adequately safeguarded to ensure that it can only be accessed for lawful purposes. If data is not also being retained for existing business purposes it cannot be used by CSPs for business purposes, for example marketing, if such a requirement is subsequently identified.

[68] Section 27(5) of the Data Protection Act 1998 states that 'the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information.' There may be other exemptions from subject access rights in specific circumstances such as where providing access is likely to prejudice crime prevention purposes.

18 Compliance

18.1 The Act places a requirement on CSPs to take all such steps for complying with any duty imposed on them under Part 4 of the Act. The duty of compliance in relation to Part 4 of the Act is enforceable in relation to conduct or a person in the UK by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988 or for any other statutory relief.

18.2 That duty can only be enforced against a person who the authorities consider may be able to provide the assistance required by the notice.

Disclosure of a retention notice

18.3 The Home Office does not publish or release identities of CSPs subject to a data retention notice as to do so may identify operational capabilities or harm the commercial interests of CSPs under a notice. This is because if criminals are aware of the capabilities of law enforcement then they may change their communications service provider accordingly.

18.4 Section 90(2) of the Act prohibits a CSP or an employee of the CSP disclosing the existence of a retention notice or the content of the retention notice to any person. That duty is enforceable by civil proceedings brought by the Secretary of State.

18.5 Section 90(4) provides for the CSP to disclose the existence of a data retention notice with the permission of the Secretary of State. Such circumstances are likely to include disclosure:

- To a person (such as a system provider) who is working with the CSP to give effect to the notice;
- To relevant oversight bodies; and
- To other CSPs subject to a retention notice to facilitate consistent implementation of the obligations.

Part 4

General Matters

19 Costs

Making of contributions

19.1 Section 225 of the Act recognises that CSPs incur expenses in complying with requirements in the Act, including the disclosure of communications data in response to requests under Part 3 of the Act and notices to retain communications data under Part 4. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.

19.2 The following sections outline the circumstances where the Government will make contributions towards the costs of complying with the Act. CSPs who are required to retain communications data will inevitably be required to disclose communications data in response to lawful requests. In those circumstances the Government will make contributions towards the costs of both retaining and disclosing the data. However, not all CSPs that are required to disclose data will be required to retain it. In those circumstances they will can only be asked to disclose data that they retain for business purposes. For such CSPs, the Government will only make contributions towards the costs of disclosing the data in response to requests under Part 3 of the Act.

Contributions of costs for the acquisition and disclosure of communications data

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

19.4 An effective and efficient response requires the timely disclosure of communications data. In this code 'timely disclosure' means that ordinarily a CSP should disclose data within ten working days of being required to do so.

19.5 It is legitimate for a CSP to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to facilitate the timely disclosure of communications data.

19.6 This is especially relevant for CSPs which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems or where, in smaller CSPs, additional resources may be required to facilitate the response to such requests.

19.7 Contributions may also be appropriate towards costs incurred by a CSP which needs to update its systems to maintain, or make more efficient, its disclosure process. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the disclosure and acquisition of communications data relating to the use of such services.

19.8 Where a CSP identifies that a request for data may result in significant costs it may discuss this with the public authority before complying with the request. This may be a relevant consideration as to whether the request is reasonably practicable.

Costs in relation to a technical capability notice

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

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

19.11 Costs that may be recovered could include those related to the procurement or design of systems required to obtain communications data, their testing, implementation, continued operation and, where appropriate, sanitisation and decommissioning. Certain overheads may be covered if they relate directly to costs incurred by CSPs in complying with their obligations outlined above. This is particularly relevant for CSPs that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems.

Contributions of costs for the retention of communications data

19.12 The above considerations may be appropriate for all CSPs that are required to disclose data. The following considerations only apply to those CSPs that are subject to a retention notice under Part 4 of the Act. They are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a data retention notice and the Act.

19.13 Any contribution towards these costs must be agreed by the Home Office before work is commenced by a CSP and will be subject to the Home Office considering, and agreeing, the solution proposed by the CSP.

19.14 These costs may include the procurement or design of systems required to retain communications data, their testing, implementation, continued operation and where appropriate sanitisation and decommissioning. Some overheads may be covered if they directly relate to costs incurred by CSPs in complying with their obligations outlined above. Costs may also include costs related to feasibility studies conducted during the period in which a CSP is being consulted prior to a retention notice being served.

19.15 This is especially relevant for CSPs that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems or where, in smaller CSPs, additional resources may be required to comply with the requirements in a notice.

19.16 Contributions may also be appropriate towards the costs incurred by a CSP to update its systems to maintain, or make more efficient, its retention process. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the use of such services.

19.17 A data retention notice must specify the level or levels of contribution to be made in respect of the costs incurred in complying with the notice. Accordingly no changes can be made to the level of contribution without the data retention notice being varied.

General considerations on appropriate contributions

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

19.19 As costs are reimbursed from public funds, CSPs should take into account value for money when procuring, operating and maintaining the infrastructure required to comply with a notice. As changes to business systems may necessitate changes to data retention and disclosure systems, CSPs should take this into account when altering business systems and should notify the Government of proposed changes which may affect the systems put in place to facilitate compliance under the Act. .

19.20 Any CSP that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

Power to develop compliance systems

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

19.22 Section 226 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop consistent systems to be used by CSPs or systems to be used by public authorities to acquire communications data. Such systems can operate in respect of multiple powers under the Act

19.23 Where such systems are developed for use in CSPs the Government will work closely with CSPs to develop systems which can be properly integrated into their networks. CSPs using such systems will have full sight of any processing of their data carried out by such systems. The Home Office should consult both the Investigatory Powers Commissioner and the Information Commissioner where relevant.

20 Referral of technical capability and data retention notices

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

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

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

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

20.5 After considering reports from the TAB and the Commissioner, the Secretary of State may decide to vary, revoke or confirm the effect of the notice.

20.6 In respect of technical capability notices, where the Secretary of State decides to confirm or vary the notice, the Investigatory Powers Commissioner must approve the decision.

20.7 Until this decision is made (in respect of data retention notices) or approved (in respect of technical capability notices), there is no requirement for the CSP to comply with the notice so far as referred. For example, if a notice covers a number of services and the referral relates to only one of those services then the CSP must continue to comply with the notice in relation to the other services covered by the notice.

20.8 Where a technical capability notice is subject to a review the duty to comply in section 63 remains in effect in relation to individual authorisations made under Part 3 of the Act.

20.9 Where a data retention notice applies to more than one CSP then only the provider(s) who refer the notice are not required to comply.

20.10 Where a referral is made in respect of a data retention notice the Information Commissioner should be notified.

21 Keeping of records

Records to be kept by a relevant public authority

21.1 Applications, authorisations, copies of notices, and records of the withdrawal of authorisations and the cancellation of notices, must be retained by the relevant public authority in written or electronic form, and physically attached or cross-referenced where they are associated with each other. The public authority should also keep a record of the date and, when appropriate to do so, the time when each notice or authorisation is given or granted, renewed or cancelled. Records kept by the public authority must be held centrally by the SPoC or in accordance with arrangements previously agreed with the Commissioner.

21.2 These records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, to carry out its functions[69]. Although records are only required to be retained for at least three years, it is desirable, if possible, to retain records for up to five years.

21.3 Where the records contain, or relate to, material obtained directly as a consequence of the execution of an interception warrant, those records must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 51 of the Act.

21.4 This code does not affect any other statutory obligations placed on public authorities to keep records under any other enactment. For example where applicable in England and Wales, the relevant test given in the Criminal Procedure and Investigations Act 1996 ('the CPIA') as amended and the code of practice under that Act. This requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor.

21.5 Each relevant public authority must also keep a record of the following information:

A. The number of applications submitted by an applicant to a SPoC seeking the acquisition of communications data (including orally);

B. The number of applications submitted by an applicant to a SPoC seeking the acquisition of communications data (including orally), which were referred back to the applicant for amendment or declined by the SPoC, including the reason for doing so;

C. The number of applications submitted to a designated senior officer for a decision to obtain communications data (including orally), which were approved after due consideration;

D. The number of applications submitted to a designated senior officer for a decision to obtain communications data (including orally), which were referred back to the applicant or rejected after due consideration, including the reason for doing so;

---

[69] The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is satisfied it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates. See section 67(5) of RIPA.

E. The number of notices requiring disclosure of communications data (not including urgent oral applications);

F. The number of authorisations of conduct to acquire communications data (not including urgent oral applications);

G. The number of authorisations to issue a notice to acquire communications data (not including urgent oral applications);

H. The number of times an urgent authorisation is granted orally;

I. The number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data;

J. The priority grading of the application for communications data;

K. Whether any part of the application relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion) (and if so, which profession)[70];

L. The number of times an authorisation is granted to obtain communications data in order to confirm or identify a journalist's source; and

M. The number of items of communications data sought, for authorisation granted (including orally)[71].

21.6 For each **item** of communications data included within a notice or authorisation, the relevant public authority must also keep a record of the following:

A. The unique reference number (URN) allocated to the application, notice and/or authorisation;

B. The statutory purpose for which the item of communications data is being sought, as set out at section 58(7) of the Act;

C. Where the item of communications data is being sought for the purpose of preventing or detecting crime or of preventing disorder, as set out at section 58(7) of the Act, the crime type being investigated;

D. Whether the item of communications data is events or entity, as described at section 237(5) of the Act, and chapter 2 of this code;

E. A description of the type of each item of communications data included in the notice or authorisation[72];

F. Whether the item of communications data relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;

G. The age of the item of communications data. Where the data includes more than one day, the recorded age of data should be the oldest date of the data sought;

---

70 See paragraphs 6.1 – 6.4 on communications data involving certain professions for more information.

71 One item of communications data is a single communications address or other descriptor included in a notice or authorisation. For example, one communications address that relates to 30 days of incoming and outgoing call data is one item of communications data.

72 The data type is to include whether the data is telephone data, whether fixed line or mobile, or internet data. It will also include a further breakdown of the data type, such as, in the case of fixed line telephone data, whether the item of communications data relates to incoming call data, outgoing call data, or both. Guidance on specific data types to be collected may be issued by, or sought from the Commissioner.

H. Where an item of data is entity data retained by the CSP, an indication of the total number of days of data being sought by means of notice or authorisation[73]; and

I. The CSP from whom the data is being acquired.

21.7 These records must be sent in written or electronic form to the Investigatory Powers Commissioner, as determined by him. Guidance on record keeping will be issued by the Commissioner. Guidance may also be sought by relevant public authorities, CSPs or persons contracted by them to develop or maintain their information technology systems.

21.8 The Investigatory Powers Commissioner will not seek to publish statistical information where it appears to him that doing so would be contrary to the public interest, or would be prejudicial to national security.

Records to be kept by a communications service provider (acquisition)

21.9 To assist the Investigatory Powers Commissioner to carry out his statutory function in relation to communications data, CSPs should maintain a record of the disclosures they have made or been required to make. This record should be available to the Commissioner and his inspectors to enable comparative scrutiny of the records kept by public authorities. Guidance on the maintenance of records by CSPs may be issued by or sought from the Commissioner's Office.

21.10 The records to be kept by a CSP, in respect of each authorisation should include:

- The identity of the public authority;
- The URN of the authorisation;
- The date the authorisation was disclosed to the CSP;
- A description of any communications data required where no disclosure took place or could have taken place; and
- The date when the communications data was disclosed to the public authority or, where secure systems are provided by the CSP, the date when the acquisition and disclosure of communications data was undertaken.

21.11 CSPs should also keep sufficient records to establish the origin and exact communications data that has been disclosed in the event of later challenge in court. CSPs should retain this data for a period of up to two years. This may comprise data that was disclosed, a copy of the response, or a digital record that could be used to validate the response but should contain no more data than is necessary to verify the authenticity of such disclosures in court[74].

---

[73] In the case of a forward facing authorisation, the number of days of data sought will often differ from the number of days of data disclosed or acquired. This is because a forward facing authorisation will often be withdrawn or cancelled at the point it has served its purpose. For example, if the purpose is to identify an anticipated communication between two suspects, the authorisation may be withdrawn subsequent to that communication being made.

[74] A digital signature is an electronic record of a disclosure and would assist the court in verification of the origin and integrity of the data throughout the acquisition, investigation and prosecution process. Where a digital signature is held there should be no need to retain the underlying data.

21.12 A requirement to delete data at the end of the period of its retention specified under a retention notice does not apply to records held for this purpose.

Records to be kept by a communications service provider (retention)

21.13 To assist the Information Commissioner carry out his statutory function in relation to the Act, CSPs must maintain a record of information that indicates whether and how they have complied with the provisions of this code. Such information must be provided to him on request.

21.14 Such records may include but are not limited to:

- Data retention & disclosure system access audit records;
- IT Health Check security reports;
- Security incident logs;
- Data retention volumes;
- Details of retained financial records (i.e. PCI-DSS implications and required exemptions);
- Data destruction records;
- Hardware (storage media) destruction records; and
- Documentary evidence to demonstrate how the CSP has fulfilled its responsibilities under chapter 16 regarding security, integrity and destruction of retained data.

21.15 Guidance on the maintenance of records by CSPs to assist with the Information Commissioner's statutory functions in relation to the Act may be issued by or sought from him.

Errors

21.16 This section provides information regarding errors, which are not considered to meet the threshold of the offence detailed at paragraph 12.7.

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

21.18 An error can only occur after a designated senior officer has granted an authorisation and the acquisition of data has been initiated.

21.19 Any failure by a public authority to apply correctly the process of acquiring or obtaining communications data set out in this code will increase the likelihood of an error occurring.

21.20 Where any error occurs in the granting of an authorisation, the giving of a notice or as a consequence of any authorised conduct – including use of the request filter, or any conduct undertaken to comply with a notice, a record should be kept.

21.21 Where an error results in communications data being acquired or disclosed wrongly, a report must be made to the Commissioner ('a reportable error'). Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, result in the individual being wrongly detained or wrongly accused of a crime as a result of that error.

21.22 In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ('recordable error'). These records must be available for inspection by the Commissioner.

21.23 'A reportable error' as set out in this code constitutes a relevant error for the purposes of section 209 of the Act (see section on serious errors beginning at paragraph 21.33).

21.24 This section of the code cannot provide an exhaustive list of possible causes of reportable or recordable errors. Examples could include:

Reportable errors

- An authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under the Act;
- Human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is acquired or disclosed;
- Disclosure of the wrong data by a CSP when complying with a notice;
- Acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation;and
- The omission of, or incorrect matches in filtered results, or the release of results that exceed specified thresholds.

Recordable errors

- A notice has been given which is impossible for a CSP to comply with and the public authority attempts to impose the requirement;
- Failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation[75];
- The requirement to acquire or obtain the data is known to be no longer valid;
- Failure to serve written notice (or where appropriate an authorisation) upon a CSP within one working day of urgent oral notice being given or an urgent oral authorisation granted;
- Where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly; and

[75] In this context seeking the disclosure of communications data unnecessarily means any failure to collate or record information already obtained which results in repeatedly obtaining the same data within the same investigation or operation. This does not restrict a relevant public authority undertaking the acquisition of communications data where necessary and proportionate, for example to extend the time frame of communications data already obtained, which may include elements of data previously obtained, or as a consequence of new evidence.

- Human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is not acquired or disclosed.

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

21.26 When a reportable error has been made and identified, the public authority which made the error, or established that the error had been made, must establish the facts and report the error to the authority's senior responsible officer and then to the Commissioner within no more than five working days. All errors should be reported as they arise. If the report relates to an error made by a CSP, the public authority should also inform the CSP and Commissioner of the report in written or electronic form. This will enable the CSP and Commissioner to investigate the cause or causes of the reported error.

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

21.28 Where a CSP discloses communications data in error, it must report each error to the Commissioner within no more than five working days of the error being discovered. It is appropriate for a person holding a suitably senior position within a CSP to do so, identifying the error by reference to the public authority's unique reference number and providing an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. Errors by service providers could include responding to a notice by disclosing incorrect data or by disclosing the required data to the wrong public authority[76].

21.29 In circumstances where a reportable error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal (see chapter 23).

21.30 The records kept by a public authority accounting for recordable errors must include details of the error, explain how the error occurred and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not reoccur. The authority's senior responsible officer must undertake a regular review of the recording of such errors.

21.31 Where material which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it is disclosed in error by a CSP, that material and any copy of it (including copies contained in or as attachments in electronic mail) should be destroyed as soon as the report to the Commissioner has been made.

21.32 Communications identifiers can be readily transferred, or 'ported', between CSPs. When a correctly completed authorisation or notice results in a CSP indicating to a public authority that, for example, a telephone number has been 'ported' to another CSP, that authorisation or notice will not constitute an error – unless the fact of the porting was already known to the public authority.

Serious errors

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

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

21.35 If the Commissioner concludes that the error has casued significant prejudice or harm to the person concerned, the Commissioner must also decide whether he considers that it is in the public interest for the person concerned to be informed of the error. In making this decision, the Commissioner must in particular consider:

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

21.36 Before making his or her decision, the Commissioner may require the public authority which has made the error to make submissions on the matters above.

Excess Data

21.37 Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority.

21.38 Where a public authority is bound by the Criminal Procedure and Investigations Act 1996 (CPIA) and its code of practice, there will be a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid authorisation. If a criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

21.39 If, having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The designated senior officer will then consider the reason(s) and review all the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. As with all communications data acquired, the requirements of the DPA and its data protection principles must also be adhered to in relation to any excess data.

Reporting of errors to the Information Commissioner

21.40 CSP are only required to report errors made in response to requests for communications data under Part 3 to the Investigatory Powers Commissioner. The Investigatory Powers Commissioner must consider whether any errors either reported or uncovered during inspections have resulted in personal data breaches that should be reported to the Information Commissioner, or whether details of the errors should be forwarded on because they are relevant to Information Commissioner's role under Part 4.

21.41 The Investigatory Powers Commissioner and the Information Commissioner should agree the circumstances under which information on errors should be forwarded.

22 Oversight

The Investigatory Powers Commissioner

22.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ('the Commissioner'), whose remit is to provide comprehensive oversight of the use of the powers contained within Parts 3 and 4 of the Act. By statute the Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work.

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

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

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

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

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

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

22.8 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to an individual who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the individual affected. Further information on errors can be found in chapter 21 of this code. The public body who has committed the error will be able to make representations to the Commissioner before they make their decision on whether it is in the public interest for the individual to be informed.

22.9 The Commissioner must also inform the affected individual of their right to apply to the Investigatory Powers Tribunal (see chapter 23 for more information on how this can be done) who will be able to fully investigate the error and decide if a remedy is appropriate..

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

The Information Commissioner

22.11 The Act requires that the Information Commissioner provides independent oversight of the integrity, security or destruction of data retained by virtue of part 4 of the Act. The role extends to all such data, irrespective of the system the data is retained in.

22.12 This code does not cover the exercise of the Information Commissioner's functions. It is the duty of any CSP subject to a notice under the Act to comply with any requests made by the Commissioner, in order to provide any information he requires to discharge his functions. The Commissioner may, for example, make requests:

- to access any relevant premises;
- for copies of relevant documentation;
- to inspect any relevant equipment or other material; or
- to observe the processing of relevant communications data.

22.13 Without prejudice to the independence of the Information Commissioner, if a CSP considers a request to be unreasonable they should refer the matter to the Home Office.

22.14 Reports made by the Information Commissioner concerning the inspection of CSPs and the security, integrity and destruction of communications data retained under the Act must be made available by the Information Commissioner to the Home Office. This can help to promulgate good practice and identify security enhancements and training requirements within CSPs. The Home Office will work with CSPs to address any recommendations made by the Information Commissioner.

22.15 Subject to discussion between the Information Commissioner and the Home Office, either may publish the inspection reports, in full or in summary, or a single overarching report to demonstrate both the oversight of the security, integrity and destruction of data and CSPs compliance with the Act. Because of the sensitivity of identifying which companies have received retention notices, any such report must be sufficiently redacted to protect the identities of the companies.

22.16 Section 90(3) of the Act prohibits the Information Commissioner or a member of his staff disclosing the existence of a retention notice or the content of the retention notice to any person without the permission of the Secretary of State.

Enforcement of integrity, destruction and security standards

22.17 The Act imposes a duty on CSPs to comply with requirements or restrictions imposed by the Act or a retention notice issued under the Act. That duty is enforceable by civil proceedings brought by the Secretary of State.

22.18 In the event of a failure to comply with the integrity, destruction and security requirements contained in the Act or in a retention notice, the Secretary of State will consider whether enforcement action is appropriate or whether to work with CSPs to address any issues identified in the first instance.

22.19 Additionally, should the Information Commissioner establish instances of failure to comply with the Data Protection Act 1998 or other relevant data protection legislation, he may take enforcement action using powers under that legislation.

22.20 Should the Information Commissioner identify any errors or issues relating to the disclosure of communications data he may take such steps as he considers necessary to bring them to the attention of the CSP. Chapter 21 of this code sets out the requirements on CSPs in relation to any such errors.

23 Contacts / Complaints

General enquiries relating to communications data retention and acquisition

23.1 The Home Office is responsible for policy and legislation regarding communications data acquisition and disclosure. Any queries should be raised by contacting:

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

commsdata@homeoffice.x.gsi.gov.uk

23.2 The Knowledge Engagement Team within the College of Policing can provide advice and guidance to police and other public authorities in relation to their obligations under communications data legislation. The Knowledge Engagement Team can be contacted at:

ketadmin@college.pnn.police.uk

Complaints

Data security, integrity and destruction

23.3 The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with these regulations. Failure to comply with this code's provisions in these areas may also engage concerns about compliance with data protection and related legislation. Any concerns about compliance with data protection and related legislation should be passed to the Information Commissioner's Office (ICO) at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

0303 123 1113

www.ico.org.uk

Acquisition and retention of communications data

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

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

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

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

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

This code of practice relates to the powers and duties conferred or imposed under Parts 3 and 4 of the Investigatory Powers Act relating to the acquisition of communications data by public authorities and its disclosure by communications service providers, and to the retention of communications data by communications service providers.

It provides guidance on:

- procedures to be followed for the acquisition of communications data;
- rules for the granting of authorisations to acquire data and the giving of notices to require disclosure of data;
- procedures to be followed for the retention of communications data;
- security principles which must be adhered to by those retaining data;
- keeping of records, including records of errors; and
- the oversight arrangements in place for acquisition and retention of communications data.

This code is aimed at:

- members of public authorities who are involved in the acquisition of communications data whether as an applicant, a single point of contact, a designated senior officer or a senior responsible officer; and
- communications service providers' staff involved in the lawful disclosure of communications data or who currently, or may in the future, retain data under the Act.