Home Office

Communications Data

DRAFT Code of Practice

November 2017

Communications Data

DRAFT Code of Practice

November 2017

Contents

Section 4: General matters

Section 1

Introduction

1 Introduction

1.1 This code of practice relates to the exercise of functions conferred by virtue of 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 telecommunications operators and postal operators. The relevant public authorities are those public authorities that can acquire communications data. They are set out in Schedule 4 to 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:

- is authorised by a warrant or order issued by a person holding judicial office; or
- deals with telecommunications operators, postal operators, or a class of such operators and can be used either:
  - in connection with the regulation of telecommunications operators, telecommunications services or telecommunication systems, or postal operators or services;[1] or
  - to acquire communications data relating to postal items crossing the United Kingdom border.

1.4 Such powers should only be used to obtain communications data from a telecommunications operator or postal operator where it is not possible for the public authority to obtain the communications data under the Act[2].

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 restrictions on disclosing personal data under relevant data protection legislation.

1.6 Sections 1, 3 and 4 of this code are relevant to telecommunications operators and postal operators who have been given a data retention notice under Part 4.

---

[1] The Office of Communications (OFCOM) 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.

[2] Section 12(3) provides that regulatory powers and powers to acquire postal communications 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 telecommunications operators and postal operators 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 IPC appointed under section 227 of the Act and by his Judicial Commissioners and inspectors. Duties under Part 4 of the Act and this code in relation to the security, integrity and destruction of data retained under a retention notice are subject to audit by the Information Commissioner. Telecommunications operators and postal operators 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, telecommunications operators and postal operators as necessary.

1.13 This code extends to the United Kingdom.

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.

2 Scope and definitions

Telecommunications operator and postal operator

Telecommunications operator

2.1 A telecommunications operator is a person who offers or provides a telecommunications service to persons in the UK or who controls or provides a telecommunication system which is (wholly or partly) 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 telecommunications operators or postal operators whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK.

2.2 Section 261(11) of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service); and section 261(13) defines 'telecommunication system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. The definitions of 'telecommunications service' and 'telecommunications system' in the Act are intentionally broad so that it remains relevant for new technologies.

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

2.4 The definition of a telecommunications operator also includes application and website providers but only insofar as they provide a telecommunications service. For example an online market place may be a telecommunications operator 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. This means that numerous businesses will be considered telecommunications operators in respect of some of their operations, even where the majority of their work is unrelated to telecommunications services or telecommunications systems. It can therefore sometimes be difficult for a relevant public authority to determine whether they need an authorisation under Part 3 of the Act to acquire the information they are interested in. The following paragraphs are intended to provide guidance for such circumstances.

When an authorisation under Part 3 of the Act is required

2.5 A large number of companies are telecommunications operators for the purposes of the Act, but they will also provide other services. It will sometimes be difficult for a relevant public authority to determine whether the information they are seeking is communications data held in relation to a telecommunications service and therefore

whether this code is relevant and an authorisation under Part 3 of the Act will be required. When information is sought from a company, the following steps are intended to assist in such considerations.

A company that solely provides a telecommunications service

2.6 Where information is sought from an operator who solely provides a telecommunications service then the data will usually be communications data and an authorisation under Part 3 of the Act will be required. If the public authority is unsure whether the information that is sought is communications data then a Single Point of Contact (SPoC) should be consulted.

A company whose primary service is a telecommunications service

2.7 Where information is sought from an operator whose primary service is a telecommunications service then unless the public authority is confident the information that is sought is not communications data, for example if it solely relates to a TV service, then a SPoC should also be consulted. Where the information is communications data an authorisation will be required and all the processes in this code should be followed.

A company where the telecommunications service is only a limited part of their offering

2.8 Where information is sought from a company for which the telecommunications service is only a limited part of their offering, careful consideration will be required to determine whether an authorisation under Part 3 is required. While most information sought from such companies will not be communications data, if the information that is sought would be communications data in some contexts (for example, telephone numbers or IP addresses) the public authority will need to consider whether the data is held in relation to the telecommunications service that the company operates or only available from a telecommunications system. If the data is held in respect of the telecommunications service or only available from a telecommunications system then an authorisation will be required and the steps in this code should be followed.[3] If the public authority is unsure how the information is held then the SPoC should be consulted.

2.9 However, if the information would be considered communications data in some contexts, is linked to a specific point in time and would have been logged automatically by a system (as opposed a person giving their phone number on an online form, for example) then, unless there is evidence that it is not appropriate, the request should be considered an application for communications data and an authorisation under Part 3 will be required. For example, a request for the IP address of someone when they registered for (or last used) an online marketplace is a request for data that is likely to only be held in respect of a telecommunications service or only available from a telecommunication system and should be treated as an application for communications data. This is because the data is likely to simply be logged automatically by the online marketplace's telecommunications system when the service is used. Whereas if the request is for any account data held in

[3] Some companies will operate a number of distinct telecommunications services, for example an online dating service may operate a telecommunications system that allows customers to communicate with each other. They may also operate a telecommunications system in the form of a server that logs users to the site.

relation to the online marketplace then that request will require a different legal mechanism, as it does not meet the requirements in Part 3.

2.10 It is possible a company, such as an online marketplace, might disclose data that would otherwise be communications data in response to a request for the account information of a customer of an online marketplace: for example, if they decided to proactively access their servers to identify all IP addresses and times the customer had used their account and to disclose that information. There is no breach of the Act in such circumstances because communications data was not requested and it must be assumed that for some business purpose the company decides that the information is stored in respect of the online marketplace, rather than the telecommunications service. Where such data is disclosed by the company, it is good practice for the person who received the data to inform the relevant public authority's SPoC so the SPoC will be able advise future applicants on how the company treats its data.

2.11 Where a relevant public authority wishes to acquire data that is both communications data and other information they will need to ensure they have lawful authority for both types of acquisition.

Other types of telecommunications operator

2.12 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. Such telecommunications services may be provided by the overall service provider or by another telecommunications operator as a partner or on their behalf. In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider e.g. the hotel, restaurant, library or airport lounges, or where there are security implications in doing so, the data may be sought from the telecommunications operator which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of communications data from such organisations, for example, where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room.

Postal operator

2.13 Section 262 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.

2.14 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

2.15 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 and will not therefore contain any content. Section 261(6)(b) makes clear that anything which is systems data is, by definition, not content. Additionally, 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 Chapters 1 and 3 of Part 6 of the Act. Further details on systems and identifying data can be found in the interception and equipment interference codes of practice.

2.16 Communications data is a subset of systems data[4]. The Act 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 (but any meaning arising from the fact of the communication or transmission of the communication is not content). That is, any systems data which would, in the absence of section 261(6)(b), be content, cannot be communications data.

2.17 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 Act and 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 Act and the Equipment Interference Code of Practice.

Communications data

2.18 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].

2.19 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.

2.20 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.

---

[4] See section 263(4)

[5] See paragraph 2.50 for the definition of content.

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

2.21 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

2.22 Communications data in relation to telecommunications operators' services and systems includes data held or obtainable by a telecommunications operator or postal operator or which is available directly from a telecommunications system and comprises four elements.

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

2.23 This data includes information about any person or entity 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.

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

2.25 Importantly this data is limited to data held or obtained by the telecommunications operator in relation to the provision of a telecommunications service – it does not include data which may be held about a customer by a telecommunications operator more generally which is not related to the provision of a telecommunications service.

2.26 For example, for a social networking 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 telecommunications service, including personal information such as political or religious interests included in profile information, is not within scope of the definition of communications data.

Data comprised in, included as part of, attached to or logically associated with a communication for the purposes of a telecommunication system that facilitates the transmission of that communication

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

2.28 This element of the communications data definition also includes data held or capable of being obtained, by the telecommunications operator which is logically

associated with a communication for the purposes of the telecommunication system by which the communication is being, or may be, transmitted. In practice this will often mean any data which is used to route or transmit a communication which the telecommunications operator holds or could obtain, for example from the network.

2.29 This might include, for example data about domain name system (DNS) requests which allow communications to be routed across the network. It also includes data that facilitates the transmission of future communications (regardless of whether those communications are, in fact, transmitted).

2.30 Only information falling within this section of the definition of communications data can be obtained directly from a telecommunication system by a public authority[7].

Data which relates to the use of a service or system

2.31 This element includes other information held by a telecommunications operator about the use of the service such as billing information.

Data which is about the architecture of a telecommunication system.

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

2.33 Part 3 of the Act does not apply to any conduct by a public authority to obtain publicly or commercially available communications data. A communications data authorisation under Part 3 is not mandatory to obtain reference data, such as mobile phone mast locations, from a telecommunications operator as there is no intrusion into an individual's rights. However, some reference data, such as details of Wi-Fi hotspots, may be commercially sensitive and an authorisation can be sought by a public authority seeking to obtain this data from a telecommunications operator where the telecommunications operator requires it.

Entity and Events Data

2.34 All communications data held by a telecommunication operator or obtainable from a telecommunication 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.

2.35 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

[7] See section 262(5)(b)

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 rank of the designated senior officer that can authorise acquisition of data reflects the differing levels of intrusiveness of the data. For example, in certain circumstances, the police can authorise access to entity data at Inspector level but events data is authorised at Superintendent level. Additionally entity data can be obtained in a wider range of crime types than events data.

2.36 There are some circumstances where a telecommunications operator will need to process events data in order to respond to a request for entity data. In such circumstances the level of authorisation required is for the type of data that is to be disclosed, rather than the type of data that is processed e.g. where a public authority wants to know the identity of a person using an IP address at a specific time and date this will be an application for entity data.

2.37 Where a public authority provides events data to a telecommunications operator as part of a request for entity data then the telecommunications operator may disclose that events data in the response to the entity data authorisation. Taking the example above, the telecommunications operator 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. This is because the public authority, by providing the events data to the telecommunications operator, has demonstrated they are already aware of the event and only intend to determine the entity involved in that event. By disclosing the events data the telecommunications operator would only be providing the public authority with information they already knew. Such disclosure is likely to occur where the telecommunications operator discloses the full record from their systems.

Entity data

2.38 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.

2.39 Examples of entity data include:

- 'subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "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 (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;

- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes[8]; and
- information about selection of preferential numbers or discount calls.

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

2.41 Some telecommunications operator may choose to retain user passwords[9] as clear text 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 communications service may only be sought under Part 3 of the Act from a telecommunications operator in the following circumstances:

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

2.42 A communications data authorisation cannot authorise a public authority to use a password obtained through that or another communications data authorisation. If a public authority wishes to use a password obtained through a communications data authorisation to access the content of stored communications or any communications service it must, in accordance with section 6(1)(c)(ii) of the Act, ensure that it has appropriate lawful authority.

Events

2.43 Events data covers information about time-bound events taking place across a telecommunication system at a time interval. Communications data is limited to communication events describing the transmission of information between two or more entities over a telecommunications service. This will include information which identifies, or appears to identify, any person, apparatus[10] 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.

2.44 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);

---

[8] 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.

[9] In many cases a telecommunications operator will actually retain a password hash rather than the password itself. When a user enters the password to use a service it is encrypted and the hash generated is checked against the hash already held by a telecommunications operator meaning the operator never needs to retain the actual password.

[10] 'Apparatus' is defined in section 263 of the Act to include 'any equipment, machinery, device (whether physical or logical) and any wire or cable'.

- 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, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- itemised telephone call records (numbers called)[11];
- itemised internet connection records;
- 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

2.45 A postal service is a service which involves one or more of the collection, sorting, conveyance, distribution and delivery of postal items and where its main purpose (or one of its main purposes) is to make available or facilitate the transmission of postal items containing communications. Communications data in relation to a postal service is defined at section 262(3) of the Act and comprises three elements.

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

2.46 This 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).

Data relating to the use made by a person of a postal service

2.47 This element of the definition of communications data in the postal context is data relating to the use made by any person of a postal service, or any part of it; for example:

- 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.

[11] 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.

Information held or obtained by a postal operator about persons to whom the postal operator provides or has provided a communications service and which relates to the provision of the service

2.48 This 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.

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

2.50 Examples of data under this element of the definition of postal communications data 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.

2.51 Postal data is defined in section 262(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.

2.52 Those public authorities that under certain conditions are able to authorise access to entity data at a lower level of seniority may also authorise access to this element of postal communications data at the same level.

Content

Telecommunications definitions

2.53 The content of a communication is defined in section 261(6) of the Act as any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of that communication.

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

2.55 When a communication is sent over a telecommunication system it can be carried by multiple operators. Each operator 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 use 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.

2.56 There are two exceptions to the definition of content (set out in section 261(6)). The first is any meaning that could be inferred from the fact of the communication. When a communication is sent, the simple fact of the communication may convey some meaning, e.g. it 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.

2.57 The second makes clear that systems data cannot be content.

Postal definitions

2.58 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. 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 and will not be content.

Web browsing and communications data

2.59 Web 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 uniform resource locators (URLs).

2.60 In order to access a webpage over the internet, key parts of a URL are normally converted from the web address format we are familiar with to numeric IP addresses, for example by means of the Domain Name System (DNS) protocol.

2.61 URLs follow a standardised structure and will always contain:

- the scheme - used to transfer the data – for web data this is commonly the http protocol;
- the host identifier, which can be a fully or partially qualified domain name or simply the host's IP address.

2.62 In order for the process of gaining access to a web address to be completed an IP address is required; this may be derived from a fully qualified domain name (FQDN). Where a host identifier only provides a partially qualified domain name (PQDN) the DNS process must generate a FQDN for the browser, or the communication will fail. Some web sites split their content across a number of servers. Because the content is split across a number of servers elements of the URL may be used to route the communication to the correct server.

2.63 These elements of a URL are necessary to route a communication to the intended recipient and are therefore communications data. Although FQDNs provide an indication of the type of content that the server being accessed contains they do not identify individual items of content and therefore are not content. The exception to the definition regarding inferred meaning ensures this.

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

- the port, which is an extended part of the IP address, and is required to make the communication process function.
- the userinfo. This includes usernames and authorisations.
- the path and optional parameters, which are similar to a file path on a computer. For example in 'socialmedia.com/profile/home' the path is /profile/home.
- the optional query parameters, identified by a '?', and fragments, identified by a '#', in the URL. These parameters contain data which helps to locate certain content but does not fit within a hierarchical path structure such as the one above.

2.65 The port and, where required to route a communication, the userinfo will be communications data.

2.66 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 communications data, and therefore can only cover those elements of a URL which constitute communications data.

Relevant communications data

2.67 A data retention notice under the Act may only require the retention of relevant communications data. Relevant communications data is defined in section 87 of the Act and is a subset of communications data.

2.68 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;

[12] See section on web browsing and communications data, paragraphs 2.59-2.66.

- 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.

2.69 The data that can be retained under a notice includes the data which would form an internet connection record (see below).

2.70 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 telecommunications operator or postal operator to correlate the above data and disclose it when required to under Part 3 of the Act. This may include, but is not limited to, customer reference numbers.

2.71 Section 87(4) of the Act ensures that a retention notice must not require the retention of third party data. Where the telecommunications operator needs the data for the functioning of a telecommunication system or where the data is retained or used for any other purpose, it is not third party data. For example, where data that would otherwise be third party data is processed and recalculated it is no longer third party data. Equally, where it is not reasonably practicable to separate the third party data from other data that is subject to the retention notice then that third party data can be retained. Determining what is third party data and whether it can be separated from other data is complex and will require careful consideration on a case by case basis as part of the consultation before a retention notice is given.[13]

2.72 A retention notice can never require a telecommunications operator or postal operator to retain the content of a communication.

Internet connection records

2.73 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 telecommunication system for the purpose of obtaining access to, or running, a computer file or program where that data is generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication. In many 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.

2.74 An ICR will only identify the service that a customer has been using. For example many social networking apps on a device maintain persistent connections to a service. Even in this case the relevant ICR will signpost the service accessed by the

[13] See paragraphs 2.79-2.83 for more information on third party data.

device, enabling the public authority to make further enquiries of the social networking provider identified from an ICR.

2.75 There is no single set of data that constitutes an ICR, as it will depend on the service and service provider concerned. The core information that is likely to be included is:

- a customer account reference – this may be an account number or an identifier of the customer's device or internet connection;
- the source IP address and port;
- the destination IP address and port – this is the address to which the person is routed 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.) although ports are often reused for different purposes; and
- the date/time of the start and end of the event or its duration.

2.76 In addition an ICR may also include, for example:

- the volume of data transferred in either, or both, directions;
- the name of the internet service or attributable server that has been connected to; and
- those elements of a URL which constitute communications data – see paragraphs 2.59 to 2.66.

2.77 Where a data retention notice is considered requiring a telecommunications operator to retain ICRs the specific data that an internet access provider may be required to retain will be discussed with the provider before the requirement is imposed[14].

2.78 The restriction on the retention of third party data applies to ICRs as it applies to other types of communications data.

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

Third party data

2.80 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

[14] See paragraph 14.11 on giving notices.

any need to see or access the full email address in order to connect the sender or recipient to the mail server.

2.81 Where one telecommunications operator is able to see or access 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 this is regarded as third party data. A telecommunications operator is considered to process data 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.

2.82 If a telecommunications operator or postal operator 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 therefore be covered by a data retention notice.

2.83 A communications data authorisation may be given for 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 telecommunications operator or postal operator need only obtain and disclose third party data where reasonably practicable to do so. Where such data is encrypted by the third party a telecommunications operator is under no obligation to decrypt such information.

Guidance on definitions

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

2.85 The Home Office may issue further guidance to telecommunications operators, postal operators or public authorities, on how the definitions in the Act apply.

Section 2

Communications data acquisition and disclosure

3 General extent of powers

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 Training should be made available to all those who participate in the acquisition and disclosure of communications data[15].

Considerations regarding necessity

3.3 The Act stipulates that conduct to be authorised or required must be necessary for one or more of the purposes set out in the Act. These are:

- in the interests of national security;
- for the applicable crime purpose;
- 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 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; or
- where a person ("P") has died or is unable to identify themselves because of a physical or mental condition to a) assist in identifying P, or b) 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.

3.4 The applicable crime purpose will depend on whether the communications data being sought is classified as entity data or events data. The definition of applicable crime purpose is found in section 60A(8) and repeated in sections 61(7A) and 61A(9). It means that where the communications data sought is wholly or partly events data the purpose must be for "serious crime" as defined in section 86(2A). In any other case the communications data must be for the purpose of preventing or detecting crime or of preventing disorder.

3.5 For the purposes of Parts 3 and 4 of the Act "serious crime", defined in section 86(2A) of the Act means: an offence for which an adult is capable of being

[15] For law enforcement, a Communications Data Professional Oversight Board will be responsible for overseeing compliance training for relevant personnel who have responsibilities set out within legislation relating to the lawful acquisition of communications data. All standards are set in accordance with legislation and codes of practice. Any advice and recommendations from the Board will be made available to all relevant public authorities

sentenced to six months or more in prison; any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal[16]; any offence committed by a body corporate[17]; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

3.6 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 the subject of a prosecution. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution, it will, with immediate effect, no longer be appropriate to obtain communications data under the Act.

3.7 The statutory purpose 'in the interests of public safety' 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.

3.8 The statutory purpose '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' can include those situations where, for example, there is serious concern for the welfare of a vulnerable person, for example, if such a person is missing.

3.9 The purposes for which individual public authorities are permitted to seek to acquire communications data are set out in Schedule 4 to the Act (and for local authorities in section 73). The authorising individual[18] may only consider necessity on grounds open to the individual public authority and only in relation to matters that are the statutory or administrative function of the 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.

3.10 Where an authorisation is granted under section 60A(1)(b)(ii) or 61(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 authorising individual must be clear that it is also required for one of the specified purposes s and the application is proportionate to what is sought to be achieved. There may be circumstances where it is appropriate to use a testing authorisation in respect of a real investigation. For example, if a telecommunications operator or postal operator has started retaining a new data type a public authority will need to begin acquiring that data to test the reliability of the telecommunications operator's

[16] See section 263(1) of the Act

[17] A body corporate is an organisation such as a company or government that is considered to have its own legal rights and responsibilities.

[18] See paragraph 4.11

or postal operator's retention systems. In such circumstances, it might be appropriate to authorise the testing in respect of a specific investigation so as not to unnecessarily infringe on the privacy of someone entirely unrelated to any investigation.

3.11 Before public authorities can acquire communications data, authorisation must be given by an authorising individual. An application for that authorisation must include an explanation of the necessity of the application.

3.12 Necessity should be a short explanation of the investigation or operation, 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.

3.13 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 sought, such as a telephone number or IP address, and how this data is related to the person and the event.

Considerations regarding proportionality

3.14 When granting an authorisation the authorising individual 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.

3.15 As well as consideration of the rights of the individual whose data is to be acquired 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.

3.16 Section 2 of the Act requires an authorising individual to have regard to the following when granting an authorisation to obtain communications data:

- whether what is sought to be achieved could reasonably be achieved by other less intrusive means,
- whether the level of protection to be applied in relation to obtaining communications data is higher because of the particular sensitivity of that information,
- 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.

3.17 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.

3.18 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[19].

3.19 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.

3.20 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.

3.21 Where an authorisation is granted for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, proportionality should be considered by assessing the potential for, and seriousness of, intrusion into any affected persons' privacy against the benefits of carrying out the proposed testing or training exercise.

3.22 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 as should any information that the applicant is aware of which might undermine the application.

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

3.24 Applications should include an explanation of how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include consideration of whether less intrusive investigations could be undertaken to achieve the objective.

3.25 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.

3.26 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.

---

[19] See section on applications for communications data relating to determining or confirming the source of journalistic information beginning at paragraph 8.23 for further information and guidance.

3.27 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 request filter (see chapter 11).

3.28 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 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".

Trade Unions

3.29 As set out in the Act, 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 given. Public authorities are permitted, for example, to apply for an authorisation against members or officials of a trade union where that is necessary for one of the statutory purposes so long as the authorisation is proportionate to what is sought to be achieved.

4 Roles

4.1 Acquisition of communications data under the Act, including national security cases and some urgent cases involves four roles:

- the applicant;
- the single point of contact
- the senior responsible officer in a public authority
- the authorising individual.

The applicant

4.2 The applicant is a person involved in conducting or assisting an investigation or operation within a relevant public authority who makes an application in writing or electronically for the acquisition of communications data.

4.3 Any person in a public authority which is permitted to acquire communications data may be an applicant, subject to any internal controls or restrictions put in place within public authorities.

The single point of contact

4.4 The SPoC is an individual trained to facilitate the lawful acquisition of communications data and effective co-operation between a public authority, the Office for Communications Data Authorisations ('OCDA') (where relevant) and telecommunications operators and postal operators. 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 unique identifier.[20] The Home Office provides authentication services to enable telecommunications operators and postal operators to validate SPoC credentials.

4.5 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.

4.6 A SPoC promotes efficiency and good practice in ensuring only practical and lawful applications for communications data are made. This encourages the public authority to regulate itself. The SPoC provides objective judgement and advice to the public authority on the application. In this way the SPoC provides a 'guardian and gatekeeper' function helping to ensure that public authorities act in an informed and lawful manner. Public authorities unable to call upon the services of an

[20] The Home Office will work with public authorities to ensure appropriate training is available, including by, where appropriate, authorising authorities to carry out training, maintaining a list of such authorities and monitoring and evaluating the training. Where this work is relevant to law enforcement, the Home Office will work with a Professional Oversight Board.

accredited SPoC should not seek to undertake the acquisition of communications data.

4.7 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, means the knowledge and experience of the SPoC in providing advice and guidance to the applicant is significant in ensuring appropriateness of any application to acquire the data necessary for an investigation.

4.8 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, subject to the safeguards in Part 3, acquire communications data under the Act to further the joint investigation.

4.9 For each individual application, the roles of applicant and SPoC will normally be carried out by two persons, depending on how a public authority uses its SPoCs. In exceptional cases 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 applicant and SPoC.

The Senior Responsible Officer

4.10 Within every relevant public authority there should be a senior responsible officer. The senior responsible officer must be of a senior rank in a public authority[21]. The senior responsible officer is responsible for:

- the integrity of the process in place within the public authority to acquire communications data;
- engagement with authorising officers in the Office for Communications Data Authorisations (where relevant);
- compliance with Part 3 of the Act and with this code, including responsibility for novel or contentious cases (see paragraph 8.51);
- oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- ensuring the overall quality of applications submitted to OCDA by the public authority (where relevant);
- engagement with the IPC's inspectors when they conduct their inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

[21] This must be at least the same rank as the designated senior officer specified in Schedule 4. Where no designated senior officer is specified the rank of the senior responsible officer must be agreed with the Home Office.

The authorising individual

4.11 Communications data applications can be authorised by three separate categories of individual depending on the circumstances of the specific case. References in this code to 'authorising individual' refer to any of the categories below. These are:

The authorising officer in the Office for Communications Data Authorisations. Section 60A of the Act confers power on the IPC to authorise certain applications for communications data. In practice the IPC will delegate these functions to his staff. These staff will sit in a body which is known as the Office for Communications Data Authorisations.

The designated senior officer: a person holding a prescribed office or rank in a relevant public authority[22] and is responsible for authorising certain applications where the requirement for independent authorisation does not apply.

A judicial commissioner: a person holding judicial office working to the IPC who is responsible for approving requests to identify or confirm journalistic sources.

4.12 Individuals who undertake the role of authorising individual 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 (see paragraphs 3.3 to 3.28, above).

4.13 The decision of an authorising individual whether or not to grant an authorisation must be based upon information presented to them in an application.

Operational independence of the designated senior officer

4.14 A designated senior officer granting authorisations under section 61 of the Act related to operations or investigations must be independent from those operations or investigations (section 63(1)). 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. Section 63 does not apply to urgent applications made under section 61A.

4.15 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[23]. This may include cases where there is an immediate threat to life or another emergency (section 63(2) of the Act).

4.16 Two further exceptions to this rule exist for applications under section 61, for national security purposes:

[22] As set out in Schedule 4 of the Act

[23] See section 63

- 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.

4.17 In all circumstances where public authorities making an authorisation under section 61 use designated senior officers who are not independent from the operation or investigation, the senior responsible officer must notify the IPC of circumstances and reasons (noting which designated senior officer granted the authorisation) at the next inspection or as otherwise required by the IPC. The details of the public authorities and the reasons such measures are being undertaken may be published and included in the IPC's report.

4.18 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.

5 Application process

Overview

5.1 The Act provides for acquisition of communications data by way of an authorisation.

5.2 This chapter sets out the application process that will apply in the vast majority of cases and involves:

- the making of an application (paragraphs 5.3 to 5.5)
- consultation with a SPoC (paragraphs 5.6 to 5.15); and
- authorisation by an authorising individual (paragraphs 5.16 to 5.27).

Making an application

5.3 The applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring communications data.

5.4 An application to acquire communications data must:

- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- 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;
- include the operation name (if applicable) to which the application relates;

- identify and explain the time scale within which the data is required[24];
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it[25];
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;
- 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; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

5.5 The application should record subsequently whether it was authorised by an authorising individual and when that decision was made. Applications should be retained by the public authority and be accessible to the SPoC.

Process that SPoC will go through

5.6 The SPoC[26] will, as appropriate:

- assess whether the acquisition of specific communications data from a telecommunications operator or postal operator is reasonably practical or whether the specific data required is inextricably linked to other data[27];
- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of telecommunications operators or postal operators;

---

[24] Public authorities, OCDA and telecommunications operators and postal operators may agree to the use of standards to indicate the appropriate timeliness for the response to lawful requirements for the disclosure of communications data, such as the Communications Data Strategy Group (CDSG) grading scheme. This scheme uses three grades: Grade 1 – an immediate threat to life; Grade 2 - Exceptionally urgent requirement for the prevention or detection of serious crime; a credible and immediate threat to national security; or a serious concern for the welfare of a vulnerable person where urgent provision of the communications data will have an immediate and positive impact on the investigation or operation; and Grade 3 – matters that are not urgent but, where appropriate, will include specific or time-critical issues such as bail dates; court dates; where persons are in custody; or where there is a specific line of investigation into a serious crime and early disclosure by the telecommunications operator or postal operator will directly assist in the prevention or detection of that crime. With Grade 1 and 2 the emphasis is on urgent provision of the communications data in anticipation of an immediate and positive impact on the investigation or operation.

[25] See section on necessity and proportionality, beginning at paragraph 3.3. This also applies to the next two bullets on collateral intrusion and unintended consequences.

[26] 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.

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

- engage with applicants to develop and implement effective strategies to obtain communications data in support of operations or investigations;
- advise on and manage the use of the request filter, specifically in relation to progress of requests through the filter and compliance by the filter with the relevant authorisation (see chapter 11);
- advise on the interpretation of the Act, particularly whether an authorisation is appropriate;
- provide assurance that authorisations are lawful under the Act and free from errors;
- consider and, where appropriate, provide advice on possible unintended consequences of the application;
- assess any cost and resource implications to both the public authority and the telecommunications operator or postal operator of communications data requirements;

5.7 Where a number of providers are involved in the provision of a telecommunications service, consultation with the public authority's SPoC will determine the most appropriate plan for acquiring data and this will be set out in the application. It is the authorising individual who ultimately decides whether to authorise the acquisition of data.

5.8 Any conduct to determine the telecommunications operator or postal operator 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.

5.9 Given the training undertaken by a SPoC and the on-going nature of a SPoCs engagement with telecommunications operators or postal operators, it is good practice to engage the SPoC to liaise with the telecommunications operator or postal operator where a public authority seeks to acquire reference data.

Exceptional circumstances where you do not need to use a SPoC

5.10 Section 76 requires that a SPoC is consulted on all applications before they are authorised unless the exceptional circumstances set out in that section apply.

5.11 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 authorisations for communications data can be given in certain limited situations.

5.12 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.

5.13 There is a requirement to ensure that, in those cases where a SPoC is not available, the authenticity of the authorisation can be or has been verified by the telecommunications operator or postal operator. 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.

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

5.15 In all circumstances where public authorities do not consult a SPoC before an application is made, the senior responsible officer must notify the IPC of circumstances and reasons at the next inspection or as otherwise required by the IPC. The details of the public authorities and the reasons such measures are being undertaken may be published and included in the IPC's report.

Authorisation of applications

5.16 Section 60A of the Act provides for the independent authorisation of communications data requests by the IPC. The Office for Communications Data Authorisations (OCDA) performs this function on behalf of the IPC. An authorising officer in OCDA can authorise any request, for any purpose from any public authority.

5.17 Section 61 provides for the authorisation of communications data requests relating to national security. Where an application for communications data is for the purpose of national security under section 61(7)(a), section 61(7)(c), or where it is an application made by a member of an intelligence agency under section 61(7)(b), an application may alternatively be authorised internally by a designated senior officer in a public authority. The designated senior officer must, except where provided for in the Act, be independent of the operation concerned (see paragraph 4.14).

5.18 A designated senior officer may also authorise a request for communications data where there is an urgent need to acquire the data because of an imminent threat to life or another emergency. See paragraphs 5.28 for further details.

5.19 Where an application relating to national security could be made under either section 60A or section 61, the decision on which authorisation route is most appropriate in any given case is a matter for individual public authorities. Public authorities who wish to use the designated senior officer route should have clear guidelines in place on when this authorisation route is appropriate and should make OCDA aware of their proposals to allow OCDA to take informed decisions about resources required to maintain a good service.

5.20 The authorising individual is responsible for considering and, where appropriate, authorising an application for communications data. It is their responsibility to consider the application and record their considerations at the time, in writing or electronically in order 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.

5.21 If the authorising individual believes the acquisition of communications data meets the requirements set out in the Act and is necessary and proportionate in the specific circumstances, an authorisation will be granted. If the authorising individual

does not consider the criteria for obtaining the data have been met the application should be rejected and/or referred back to the SPoC and the applicant.

5.22 There may be circumstances where the authorising individual, having read the case set out by the applicant and the considerations of the SPoC, will want to comment why it is necessary and proportionate to obtain the data despite a significant amount of data being acquired.

5.23 When considering proportionality, the authorising individual should apply particular consideration to unintended consequences. Specific additional proportionality issues relating to use of the request filter are detailed at paragraph 11.9.

5.24 Authorising individuals may only grant authorisations for the purposes specified in the Act, and only in respect of types of communications data that the relevant public authority is permitted to apply for, as set out in Schedule 4 to the Act.

5.25 Particular care must be taken by authorising individuals 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[28]. 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.

5.26 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 telecommunications operators and postal operators 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.

5.27 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 telecommunications operator or postal operator to provide such assistance outside of its normal business practice.

Urgent granting of an authorisation

5.28 A designated senior officer in a public authority can grant an authorisation for specified purposes in cases where there is an urgent need to acquire the data (section 61A). Public authorities should, where relevant, inform the Office for Communications Data Authorisations (OCDA) of how much they expect to use this process to allow OCDA to make appropriate staffing arrangements.

---

[28] The regional representative of the Data Communications Group Evidence Group will be in a position to offer additional advice to SPoCs where investigations or operations in their public authority are considering the acquisition of such data.

5.29 The use of urgent processes 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 can be undertaken using the urgent process. It must be clear in each case why it was not possible, in the circumstances, to use the standard process.

5.30 If as a matter of urgency, an authorising individual decides, having consulted the SPoC, that the urgent granting of an authorisation is appropriate, the authorised conduct should be undertaken as soon as practicable after the making of that decision.

5.31 Circumstances in which an urgent authorisation may be appropriate include but are not limited to:

- 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 urgent operational requirement where, within no more than 48 hours of the urgent authorisation being granted, the acquisition of communications data will directly assist the prevention or detection of the commission of a serious crime[29] or the making of arrests or the seizure of illicit material, or 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.
- A situation where there has been a loss of life or serious harm to an individual, or where a person is otherwise unable to identify themselves, and the acquisition of communications data will assist with locating the next of kin of the affected individual where there are no other methods to locate the next of kin

5.32 In urgent circumstances where it would not be reasonably practicable to complete the written authorisation process in the time available to meet an operational or investigative need, an application for the grant of an authorisation may be made by an applicant and approved by an authorising individual orally.

5.33 Where a public authority is using section 61A to internally authorise an application, section 63 of the Act does not apply.

5.34 Particular care must be given to the use of the urgent process orally. When authorisation is given orally, the SPoC, when relaying service of the oral authorisation to the telecommunications operator or postal operator, must make a note of the time, provide a unique reference number for the notice and the name (or identifier) and contact details of the SPoC and, if required by the

[29] See section 263(1) of the Act, with paragraph 6 of Schedule 9, which provides the general definition of serious crime in the Act. This is considered the appropriate threshold where data is acquired through urgent processes.

telecommunications operator or postal operator, their unique identifier. Where telephone numbers (or other identifiers) are being relayed, the relevant number must be read twice and repeated back by the telecommunications operator or postal operator to confirm the correct details have been taken.

5.35 Written notice must be given to the telecommunications operator or postal operator retrospectively within one working day[30] of the oral authorisation being given. Failure to do so will constitute an error which may be reported to the IPC by the telecommunications operator or postal operator and must be recorded by the public authority (see the section on errors in chapter 21, Keeping of records, for more details).

5.36 After the period of urgency[31], a separate written process must be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the SPoC will 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 authorising individual and the actions taken in respect of the decision(s).

5.37 In all cases where urgent authorisation has been granted, an explanation of why the urgent process was undertaken must be recorded.

Refusal to grant an authorisation

5.38 Where an authorising individual does not consider the acquisition of communications data specified in the application to be necessary and proportionate they may either seek further information from the applicant or refuse the request.

5.39 Where a request is refused by an authorising officer in OCDA, the public authority has three options.

- Not proceed with the request
- Resubmit the application with a revised justification and/or a revised course of conduct to acquire communications data.
- Resubmit the application with the same justification and same course of conduct seeking a review of the decision by OCDA. A public authority may only resubmit an application on the same grounds to OCDA where the senior responsible officer or a person of equivalent grade in the public authority has agreed to this course of action. OCDA will provide guidance on its process for reviewing such decisions.

5.40 It is a matter for public authorities to decide what, if any, internal review mechanism exists for circumstances where a designated senior officer refuses to grant an authorisation.

---

[30] 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.

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

6 Authorisations

6.1 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; and/or
- the giving of a notice - allowing the public authority to require by a notice a telecommunications operator to obtain and disclose the required data.

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

- there is an agreement in place between a public authority and a telecommunications operator or postal operator to facilitate the secure and swift disclosure of communications data. Many telecommunications operators and postal operators have auditable acquisition systems in place to ensure accurate and timely acquisition of 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 public authority considers there is a requirement to identify a person to whom a service is provided but the specific telecommunications operator or postal operator has yet to be conclusively determined as the holder of the communications data.

6.3 An authorisation to give a notice may be appropriate where a telecommunications operator or postal operator is known to be capable of disclosing (and, where necessary, obtaining) the communications data (for further detail see paragraphs 6.19- 6.29).

6.4 Authorisations are not served upon a telecommunications operator or postal operator, although there may be circumstances where a telecommunications operator or postal operator 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 by the issuing of a notice to the operator. Where a telecommunications operator or postal operator has provided a system to facilitate the secure and swift disclosure of communications data, the fact that a request is received from an authenticated SPoC acting for a relevant public authority, or from a secure system of a relevant public authority or of the Secretary of State, shall be taken as adequate assurance that a lawful authorisation exists when the following additional information is provided:

- the unique reference number (URN) of the authorisation;

- the date when the authorisation was granted;
- a description of the communications data to be disclosed and, where relevant, the period of time the authorisation is intended to cover; and
- where appropriate, provide an indication of any time periods within which the data needs to be obtained.

6.5 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);
- specify the purpose for which the conduct is authorised, by reference to a statutory purpose under of the Act;
- include a unique reference number;
- specify the identity, rank or position (or unique identifier) of the authorising individual granting the authorisation.
- Where applicable, confirm in writing that a SPoC has been consulted on this application;
- record the date and, when appropriate to do so, the time when the authorisation was granted;
- specify when 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 acquiring ICRs, specify whether any threshold for the number of results returned is set which would prevent any portion of records being disclosed; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

6.6 In addition, an authorisation[32] to give a notice must:

- specify the operator to whom the notice applies and the nature of requirements to be imposed;

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

- identify the public authority;
- specify or describe the person(s) to whom the data is to be, or may be, disclosed or how to identify such person(s); and
- confirm whether a telecommunications operator or postal operator may disclose the existence of this requirement, or any related pursuant authorisation or notice, to a customer or other individual.

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

6.8 When drafting authorisations within the meaning of sections 60A and 61 of the Act, the authorising individual must ensure, where possible, the description of the required data corresponds with the way in which the telecommunications operator or postal operator processes, retains and retrieves its data for lawful disclosure. Telecommunications operators and postal operators 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.

6.9 Some telecommunications operators or postal operators permit the lawful acquisition of communications data by SPoCs via secure auditable communications data acquisition systems. Where a SPoC has been authorised to obtain data from such a system, but concludes that the data cannot be acquired directly, the SPoC may provide the telecommunications operator or postal operator with details of the authorisation in order to seek disclosure of the required data.

6.10 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.

6.11 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 the subject of an investigation or operation is identified from intelligence to be using a specific communications service;
- a victim, a witness or a person who is the subject of an investigation or operation has used a public payphone[33];
- 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 public authority to be using a specific communications 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); or
- 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.

[33] 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.

6.12 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.

6.13 At the time of granting an authorisation of conduct to acquire communications data or to give a notice in order to obtain specific events data, an authorising individual 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.

6.14 At the time of granting an authorisation of conduct to acquire communications data or to give a notice in order to obtain specific events data, an authorising individual 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 telecommunications operator or another telecommunications operator to query their events data information, for example:

- the telecommunications operator does not collect information about the customer within their customer information system but retains it in its original form as events data; or
- where evidence or intelligence indicates there are several telecommunications operators involved in routing a communication and there is a requirement to establish the recipient of the communication.

6.15 This process could be used to obtain consequential events data relating to the number of a person called by a high risk missing person for instance, where it is suspected that the missing person may be going to meet a person as yet unidentified, the purpose being to identify and locate that person; and thus, the missing person.

6.16 It is the duty of the senior responsible officer in a public authority to ensure that the public authority makes available to the SPoC and the authorising individual 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[34].

6.17 The SPoC would normally be the person who takes receipt of any communications data acquired from a telecommunications operator or postal operator 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 be stored and handled in accordance with duties under relevant data protection legislation[35].

6.18 Ordinarily it will be a SPoC who seeks to acquire data from a telecommunications operator or postal operator using a secure system. In circumstances where an operator is approached by a person who cannot be authenticated and who seeks to obtain data under the provisions of the Act, the telecommunications operator or postal operator may refuse to comply with any apparent requirement for disclosure of data until the authenticity of an authorisation is confirmed.

Notices in pursuance of an authorisation

6.19 The giving of a notice is appropriate where a telecommunications operator or postal operator 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 telecommunications operator or postal operator to obtain any communications data, if that data is not already in its possession.

6.20 The decision to authorise the issuing of a notice must be based on information presented in an application.

6.21 Once the authorising individual has authorised the giving of a notice, it will be given to a telecommunications operator or postal operator in writing[36] or, in an urgent situation, communicated to the telecommunications operator or postal operator orally.

6.22 The notice should contain enough information to allow the telecommunications operator or postal operator to comply with the requirements of the notice.

6.23 A notice must:

- 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);

---

[34] 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.

[35] See chapter 13 for further details of data protection safeguards.

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

- specify the requirements being imposed and the telecommunications operator or postal operator on whom the requirements are being imposed;
- 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);
- include a unique reference number and identify the public authority[37][38];
- specify the name (or unique identifier) of officer giving the notice;
- be given in writing or, if not, in a manner that produces a record, within the public authority, of its having been given;
- record the date when the giving of a notice was authorised by the authorising individual;
- where appropriate, provide an indication of any urgency or time within which the telecommunications operator or postal operator is requested to comply with the requirements of the notice;
- include an explanation that compliance with the notice is a requirement of the Act unless the notice is cancelled. A telecommunications operator or postal operator 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 telecommunications operator or postal operator to, where necessary, confirm the notice is authentic and lawful; and
- if permission has been given, confirm the telecommunications operator or postal operator may disclose the existence of this requirement, or any related pursuant authorisation or notice, to a customer or other individual.

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

6.25 A telecommunications operator or postal operator is not required to do anything under a notice which it is not reasonably practicable for it to do[39].

6.26 A notice may only require a telecommunications operator or postal operator to disclose the communications data to the public authority. This will normally be to the public authority's SPoC.

6.27 Ordinarily the telecommunications operator or postal operator should disclose, in writing or electronically, the communications data to which a notice relates within agreed service levels[40] or, where there are no agreed service levels not later than the end of the period of ten working days from the date the notice is served upon the telecommunications operator or postal operator.

---

[37] 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.

[38] Where a relevant public authority is in a collaboration agreement, only the details of the public authority of which the officer giving the notice belongs are necessary.

[39] See section 66(3) of the Act.

[40] Defined service levels may be agreed between the Secretary of State and the telecommunications operator or postal operator, for example where a retention notice includes requirements to provide for data to be transmitted efficiently and effectively in response to requests.

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

6.29 Section 85 of the Act provides that where a notice under Part 3 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).

7 Duration, renewals and cancellations

Duration of authorisations and notices

7.1 An authorisation becomes valid on the date upon which the authorisation is granted. It is then valid for a maximum of one month[41]. This means the conduct authorised should have been commenced, which may include the giving of a notice, within that month.

7.2 Any notice given under an authorisation remains in force until complied with or until the authorisation under which it was given is cancelled (see paragraph 7.12).

7.3 All authorisations should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s)[42]. 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[43]. 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 authorising individual. 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'.

7.4 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.

7.5 Authorising individuals 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 telecommunications operator or postal operator(s).

Renewal of authorisations

7.6 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.

7.7 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 reasons for seeking

---

41 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.

42 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.

43 In the case of IP data, any timings must include an explicit indication of which time zone applies to those timings.

renewal should be set out by an applicant in an addendum to the application upon which the authorisation being renewed was granted.

7.8 Where an authorising individual is granting a further authorisation to renew an earlier authorisation[44], they should:

- Consider 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

7.9 A designated senior officer who has granted an authorisation under section 61 or 61A of the Act must cancel it if, at any time after the granting of the authorisation[45], 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 by the designated senior officer.

7.10 Where an authorisation has been granted by an authorising officer under section 60A it may be cancelled at any time by the public authority or OCDA and must be cancelled if, at any time after the granting of the authorisation, 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.

7.11 In practice, it is likely to be the public authority that 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 authorising individual who granted the authorisation.

7.12 A notice given 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 telecommunications operator or postal operator should be undertaken by the SPoC in a public authority[46].

7.13 Cancellation of an authorisation granting the giving of a notice reported to a telecommunications operator or postal operator must:

- identify, by reference to its unique reference number, the notice being cancelled; and

---

[44] This can include an authorisation that has been renewed previously.

[45] This can include a renewed authorisation.

[46] 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 telecommunications operator or postal operator (or arrange for their notification) that the notice imposed under an authorisation is cancelled where that person has the earliest opportunity to do so.

- record the date and, when appropriate to do so, the time when the notice was cancelled.

7.14 Where the authorising individual who authorised the giving of the notice to the telecommunications operator or postal operator is no longer available, this duty should fall on a person who has temporarily or permanently taken over the role.

7.15 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.

7.16 When it is appropriate to do so, a telecommunications operator or postal operator should be advised of the cancellation of an authorisation, for example where details of an authorisation have been disclosed to a telecommunications operator or postal operator.

8 Further restrictions and requirements in relation to applications

Local authority procedures

8.1 The National Anti-Fraud Network (NAFN) is hosted by Tameside Metropolitan Borough Council.

8.2 In accordance with section 73 of the Act, all local authorities who wish to acquire communications data under the Act must be party to a collaboration agreement. In practice this means they will be required to become members of NAFN and use NAFN's shared SPoC services. Applicants within local authorities are therefore required to consult a NAFN SPoC throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to the local authority ensuring it acts in an informed and lawful manner.

8.3 Such collaboration agreements are required to be certified by the Secretary of State in accordance with section 73(3)(c). Where a collaboration agreement is considered to both meet the needs of those authorities' party to it and to assist in the effective application of the relevant provisions and safeguards detailed in the Act, including in relation to the factors listed in the section on collaboration agreements below, the Secretary of State will certify the agreement, therefore allowing the relevant local authorities to acquire communications data.

8.4 Certified collaboration agreements will be subject to review by the Secretary of State at least every three years. Authorities' party to the collaboration agreement are required to notify the Secretary of State of any changes which may necessitate an earlier review.

8.5 In addition to being considered by a NAFN SPoC, the local authority making the application must ensure someone of at least the rank of the senior responsible officer in the local authority is aware the application is being made before it is submitted to an authorising officer in OCDA. The local authority senior responsible officer must be satisfied that the officer(s) verifying the application is (are) of an appropriate rank and must inform NAFN of such nominations. Where the verifying officer is employed by a local authority other than that which requires access to communications data, the verifying officer must also be of an appropriate rank.

8.6 NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

8.7 A local authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

Communications data involving certain professions

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

8.9 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 an authorising individual 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.

8.10 Section 2 of the Act makes clear that public authorities and OCDA must have regard to whether the level of protection to be applied in relation to any acquisition of communications data is higher because of the particular sensitivity of that information. Examples of sensitive information include but are not restricted to legally privileged material, confidential journalistic material, the identity of a journalist's source, and communications between a Parliamentarian and their constituent.

8.11 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 a relevant legislature, or ministers of religion. That such an application has been made must be recorded (see chapter 24 on keeping of records for more details), including recording the profession, and, at the next inspection, such applications should be marked for the IPC's attention.

Applications for communications data relating to journalists and their sources

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

8.13 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.

8.14 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.

8.15 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 the time of the application. 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.

8.16 Where a public authority 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 8.28).

8.17 Applications for communications data in relation to journalists and their sources may still be made but public authorities and authorising individuals will want to take particular care in preparing and authorising 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 and authorising individuals correctly apply the process set out in this chapter.

8.18 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.

8.19 Where the purpose of an application is to identify or confirm the identity or role of an individual as a source of journalistic information, Judicial Commissioner approval must be sought prior to the acquisition of the communications data taking place, other than where there is an imminent threat to life. Where an application relates to journalists but 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.

8.20 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 authorisations are given 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 approval.

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

8.22 Where appropriate, public authorities should seek advice on the overarching application of these provisions from the Home Office, the Investigatory Powers Commissioner's Office ('IPCO') and their own legal team. In addition, where an application may be considered novel or contentious or authorising individuals should follow the processes in set out at paragraph 8.48 onwards.

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

8.23 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 and the authorising officer in the independent body must consider whether there is another overriding public interest which justifies any interference with this right.

8.24 Where an authorising individual 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 authorised it under section 77 of the Act.

8.25 Public authorities that are required to have applications for communications data authorised by OCDA by virtue of section 60A of the Act should take account of the considerations set out in this section before submitting the application to OCDA for authorisation. Once OCDA has authorised the request for communications data, they will seek the approval of the decision by a Judicial Commissioners before responding to the public authority except where there is an imminent threat to life (see paragraph 8.35 for further detail).

8.26 Public authorities authorising communications data applications internally by virtue of sections 61 or 61A of the Act must submit an application to a Judicial Commissioner for approval after it has been authorised by a designated senior officer except where there is an imminent threat to life (see paragraph 8.33 for further detail)[47].

8.27 In deciding whether to approve an application 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.

8.28 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 have regard 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.

8.29 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 approval by a Judicial Commissioner.

[47] An application under section 61A may be made in cases where there is emergency other than a threat to life.

8.30 The requirement for Judicial Commissioner approval applies to an application 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.

8.31 Public authorities should give careful consideration before seeking to acquire 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 pursuant to a statutory purpose under Part 3 and where it is considered that there is a public interest in making such an application which overrides the public interest in source protection. Judicial Commissioner approval is required in such cases.

8.32 In addition to the requirements detailed in Part 3, 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.

8.33 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.

8.34 Each public 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 24 on keeping of records for more details). At the next inspection, such applications should be specifically marked for to the IPC's attention.

Threat to life exception

8.35 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 Commissioner approval. If, and only if, there is believed to be an immediate threat to life, such that a person's life might be endangered by the delay inherent in the process of obtaining Judicial Commissioner approval the authorisation may take effect without such approval.

8.36 Examples of situations in which Judicial Commissioner approval may not be required due to an immediate threat to 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.

8.37 Such applications must be notified to the IPC as soon as reasonably practicable, as agreed with the IPC. Where an application is not for national security purposes it must also be notified to OCDA where an application has been authorised internally.

8.38 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 Commissioner approval should be sought in the normal way.

Applications relating to journalists where the purpose is *not* to identify or confirm a journalistic source

8.39 The requirement for Judicial Commissioner approval 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. However, the application may still be sensitive and all those involved in it should proceed with care.

8.40 The following bullets 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 authorising individuals 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 8.46). As this is a sensitive and often complex issue and the protection of Article 10 rights is crucial, it is important that authorising officers proceed with caution and seek additional advice if there is any doubt as to whether Judicial Commissioner approval is required.

- where the journalist is a victim of crime and it is clear that their profession and sources are not relevant to the investigation, Judicial Commissioner 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 Commissioner 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.

- where the journalist, identified source, or suspected source is suspected of committing a crime, Judicial Commissioner 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. Equally, Judicial Commissioner approval may not be required 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 Commissioner 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 Commissioner approval may not be required

8.41 Where an investigation is conducted to prove criminal conspiracy between a journalist and their source, and the journalist-source relationship is already confirmed, Judicial Commissioner 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 Commissioner approval may not be required. 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 advice.

8.42 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 but:

- will likely result in the incidental and unintended identification or confirmation of a source (collateral intrusion into journalist sources); or

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

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

- subscriber checks are authorised 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.

8.44 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.

8.45 The IPC is required to include in his annual report information about the operation of the safeguards in the Act and this code in relation to sources of journalistic information.

Novel or contentious acquisition

8.46 In recognition of the capacity of modern communications data to produce insights of a highly personal nature, public authorities must take particular care where it is considered that a communications data application is novel or contentious. However, it is important to recognise that what might be considered novel or contentious to one public authority might be more routine for another. The following examples might, depending on the specific circumstances, 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.

8.47 While such applications could be novel or contentious that does not preclude them from taking place but it is important that the proper consideration set out below is given.

8.48 For guidance on how applications for communications data relating to a journalist or their source may be considered novel or contentious, please see the section above.

8.49 Where the public authority intends to require a telecommunications operator or postal operator to undertake an action which of itself is novel or contentious, for example a new technical method of data acquisition, the SPOC should consult the operator concerned.

8.50 A public authority and OCDA may seek the advice of a Judicial Commissioner before considering whether to embark on a course of action to acquire communications data that could be considered novel or contentious. Such advice may be sought in relation to a single application to an issue of principle that may be relevant to a number of future applications.

8.51 The public authority must record the views of OCDA or Judicial Commissioner. It is the responsibility of the Senior Responsible Officer to maintain this record and a public authority should check against this information before seeking advice. This advice may be shared between public authorities to inform consideration of future applications.

8.52 Where a public authority makes an application to OCDA that it considers to be novel or contentious this fact should be flagged in the application. Any relevant previous advice from OCDA or a Judicial Commissioner should be included in the application. In considering the application the authorising officer in OCDA may discuss the case with a Judicial Commissioner.

8.53 Where a designated senior officer is considering a request for communications data that they consider to be novel or contentious they must seek advice from OCDA or a Judicial Commissioner before authorising the application. Where the designated senior officer proceeds against a recommendation from OCDA or a Judicial Commissioner the reasons for doing so must be recorded and these cases flagged to the Commissioner at their next inspection.

8.54 Where the designated senior officer has reasonable doubt as to whether an application they have been asked to authorise is novel or contentious, they should consider seeking guidance from the OCDA or a Judicial Commissioner before deciding how to proceed.

8.55 In urgent cases, such as threat to life or the interests of national security in a particular investigation, it may not be possible for the designated senior officer to seek the opinion of OCDA or a Judicial 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 relation to any ongoing conduct under the authorisation and in relation to future applications of a similar nature.

Public authority collaboration agreements

8.56 Any public authority may participate in a collaboration agreement, by which a SPoC of the supplying authority is put at the disposal of the subscribing authority. 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).

8.57 Public authorities must notify the Home Office of any plan to enter into a collaboration agreement. Before entering into an 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;
- whether 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.

8.58 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 8.57;

- the number and nature of applications made by a public authority; and
- the nature and function of the public authority concerned.

8.59 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 IPC notified.

9 Considerations in relation to the acquisition of internet data

Internet connection records

9.1 Under certain circumstances, an authorising individual may grant an authorisation to obtain data which constitutes or requires the processing or disclosure of an internet connection record (ICR) (see paragraph 2.72 for the definition of an ICR). Subject to paragraph 2.35 any application that involves the disclosure of ICRs must be authorised as events data.

9.2 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 authorising individuals 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.

9.3 Section 62 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 under Part 3 for the purpose of identifying:

- the user of an internet service (either the person or apparatus);
- the internet communications services[48] a device or person is using, such as messaging applications;
- the internet services[49] a device or person 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 a device or person is using – for example to book travel or look at online mapping services.

9.4 An application to acquire ICRs may relate to one or more of these ‘investigative purposes’.

9.5 The Act applies important restrictions when the statutory purpose for which ICRs are acquired is for “the applicable crime purpose”. In these circumstances ICRs can only be acquired

[48] 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, instant messaging services, internet telephony services, social networking and web forums.

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

for the prevention and detection of serious crime as defined in s86(2A) of the Act but where the offence attracts a prison sentence of at least 12 months (as opposed to six months which is the case for other types of communications data);

9.6 The crime threshold does not apply to applications made for the investigative purpose of identifying the sender of an online communication (section 62(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 telecommunications operator could be asked a number of different questions, for example who was using an IP address at a particular date/time, which of its customers accessed this server at a particular date/time or which of its 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).

9.7 Applications may be made by the public authority for the purpose of identifying:

- the internet communications service used by a device or person, and when and how it is used;
- internet services used to access or make available illegal material; or
- what other internet services a device or person is using, and when and how they are used.

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

9.9 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 device or individual 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.

9.10 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.

9.11 A public authority might seek ICRs in order to identify possible access to illegal information when seeking, for instance, to identify whether a person suspected of 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 to which website a person has uploaded illegal images.

9.12 A public authority might seek ICRs in relation to internet services more generally when seeking, for instance, to identify how and when 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.

9.13 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 60A(7), 61(7) and 61A(7) of the Act. For further information see paragraphs 21.39 – 21.41 on excess data.

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

9.15 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. For example, 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 acquiring the data is appropriate.

Identifying the sender of an online communication

9.16 Internet protocol address resolution (IPAR) is necessary to identify the sender of an online communication, where the public authority is in possession of a source IP address related to a communication of interest and needs to determine the customer linked to this address. There is often a pressing need for such requests to identify individuals online, for example in terrorism and child abuse investigations. 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 and balance these against the operational requirements.

9.17 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, or to the internet access point to which their device is connected;
- 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.

9.18 The 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. In most cases, the IP address from which the communication originated is the source IP address, by which it is received is the destination IP address[50].

9.19 In order to enable the telecommunications operator to resolve a source IP address to a customer the public authority must provide a minimum of one source IP address and one date/time or range of 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 specific device operated by an individual, not to a destination device (e.g. a server).

9.20 However, where IP addresses are shared between network customers, providing just the source IP address and the time of the communication will often not be sufficient for a telecommunications operator to resolve the address to an individual customer. Public authorities should therefore ensure they include any other data that is available to them with the application. For example, if there are more IP addresses and times (or time ranges) which they believe relate to the same device or person then that data should also be provided to the telecommunications operator. Other examples of data types include:

- destination IP address (if possible with the Fully Qualified Domain Name);
- port numbers;
- service identifiers;
- user equipment identifiers (e.g. type of communication equipment used, such as an IMSI number for a mobile telephone);

9.21 Where public authorities need to resolve IP addresses, internet connection record data will frequently be the only additional data that is available. This is because they will already know the internet service that has been used by the device or person which they are trying to resolve. For example, if someone posts a bomb threat to an online blog, the blog's access records may provide the police with both the source IP address allocated to the user who posted the threat, and details about the server hosting the blog, such as the IP address of the server. In such circumstances, the police should provide both these IP addresses, plus any other information the blog records provide such as port numbers used, to the telecommunications operator as this will increase the likelihood that the telecommunications operator will be able to accurately match these details to an individual customer.[51]

9.22 Where a public authority provides internet connection record data, such as a destination IP address, to a telecommunications operator in order to resolve a source IP address that request will require the telecommunications operator to process internet connection records and will therefore be considered under Condition A in section 62 concerning restrictions in relation to internet connection

[50] There will be at least three IP addresses associated with any internet communication. However, at the most basic level the source and destination IP address, as described in this paragraph, will be the most relevant to identifying the sender of online communications.

[51] Paragraph 2.36 explains that the data requested, rather than processed by the telecommunications operator, is the only issue relevant to the authorisation level.

records. Where the public authority is aware that the telecommunications operator allocates multiple customers the same IP address then, where possible, the internet connection record data should be provided by the public authority to the telecommunications operator.[52]

9.23 In cases where an IP address may only be allocated to a particular user in conjunction with other users, an authorisation for IPAR data may return a large data set to the public authority. As an authorising individual may not know in advance how large that return will be, it is important to consider the proportionality and potential collateral intrusion of such applications.

9.24 In addition to the standard authorisation procedure for communications data applications the following additional steps should be taken when seeking to identify the sender of an online communication:

- the applicant should consider what data is available to them and base their application on those elements of data which will enable the telecommunications operator to make the most appropriate 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 telecommunications operator may make the most appropriate 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 authorising individual must take account of advice provided by the SPoC as to an appropriate strategy for the acquisition of IPAR data in each case;
- The authorising individual should consider whether to specify that data should only be returned where it can be linked to one individual or whether larger data sets may be returned. The authorising individual 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;
- if the SPoC considers that data may be returned that links to more than one individual, they must, though consultation with the telecommunications operator, provide the authorising individual with guidance as to the amount of data that is likely to be disclosed; and
- the authorising individual 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

[52] The telecommunications operator may disclose the internet connection record data back to the public authority when it discloses the user of the source IP address in question (see paragraph 2.37 for further details on where a telecommunications operator may disclose data originally provided by the public authority).

negatives' where individuals are ruled out of a case because they did not appear in a particular data set should also be considered.

9.25 The considerations above will also apply to authorisations where the public authority does not have an IP address but wishes to determine the individual that carried out a certain action online. For example, if a public authority suspects an internet service is being used to share child abuse imagery it may be appropriate to determine all users of the service over the specified timeframe.

10 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

10.1 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. Sections 60A(7), 61(7) and 61A(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.

10.2 Often a 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.

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

10.4 Under the Act communications data may also be obtained and disclosed in serious welfare cases where it is necessary within the meaning of section 61(7)(e) and 61A(7)(c) 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)

10.5 The Act regulates the acquisition and disclosure of communications data for the statutory purposes set out in sections 60A(7), 61(7) and 61A(7). The Communications Act 2003 also requires certain telecommunications operators to provide communications data to the emergency services following an emergency call made to 999 and 112 emergency numbers. Further details in relation to handling 999 and 112 calls are contained within the Public Emergency Communications Service Code of Practice.

10.6 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.

10.7 The Public Emergency Communications Services Code of Practice provides that telecommunications operators 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. Whilst telecommunications operators and the emergency operator will seek to assist in identifying the location of the incident being reported, it remains the responsibility of the emergency services control room staff to obtain adequate address information from the caller to locate the incident.

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

10.9 Telecommunications operators 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. Emergency services should be aware that communications data may not always be available for disclosure by the telecommunications operator depending on the particulars of the communications service used to make the call.

10.10 If the emergency service control room has reason to doubt the address provided for a fixed-line number by the emergency operator (from what the caller has said) then they can contact the Operator Centre in the normal manner and ask for the address to be checked.

10.11 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 one hour from the termination of the 999/112 call.

10.12 It is appropriate for the emergency service or emergency operator to require the telecommunications operator 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 telecommunications operator, 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 information about the location of the caller at the time of the emergency call or a new location the caller has moved to, if it is within the one hour period.

10.13 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.

10.14 Some telecommunications operators 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, only during the emergency period.

10.15 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.

10.16 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.

10.17 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.

10.18 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.

10.19 Increasingly, members of the public are using non-emergency numbers to request assistance. For instance a caller might dial either 101 or 111 or other relevant services to seek non-emergency assistance). In some circumstances the call handler may consider it more appropriate that an emergency response is made for instance when the health of the enquirer suddenly deteriorates or a suspect returns unexpectedly to the scene of a crime. In such circumstances the one hour emergency period and related provisions detailed above apply, even though the number dialled was not an emergency number.

10.20 The Act does not seek to regulate either the actions of the call handler or the provision of data by the telecommunications operator.

Malicious and nuisance communications

10.21 Upon receipt of a complaint concerning malicious and nuisance communications a telecommunications operator or postal operator may retrieve and retain relevant specific data that, if appropriate, can be disclosed to the police later.

10.22 Where the complainant reports a matter to the police that has been previously raised with the telecommunications operator or postal operator, any data already collated by the telecommunications operator or postal operator may be disclosed to the police SPoC under the provisions of relevant data protection legislation. However subsequent police investigation may require the acquisition or disclosure

of additional communications data from the complainant's telecommunications operator or postal operator or other telecommunications operators or postal operators under the provisions of the Act.

10.23 The telecommunications operator or postal operator may choose to disclose data to its own customer relating to the source of the malicious or nuisance communications, but must ensure that the disclosure complies with the any relevant data protection legislation or any future data protection legislation.

10.24 For guidance on hoax emergency calls please see para 10.16.

11 The request filter

11.1 The request filter will provide an additional safeguard in relation to 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.

11.2 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.

11.3 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 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.

11.4 The request filter will be available to all public authorities.

Authorisations

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

11.6 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.

11.7 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 a large number of people

are likely to be in both Brighton Station at 07.30 on a Monday and London Victoria at 09.00 the following Thursday.

11.8 The authorising individual, 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 telecommunications operators or postal operators; and
- the data to be disclosed to the applicant by the request filter.

11.9 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 subsequent communications data authorisations or other means. For example, if the question to the request filter is 'which device was in location A at time N and location B at time M', it may be possible to evidence that any devices identified were indeed in the specified locations through a subsequent communications data authorisation seeking the locations of those identified devices at times N and M.

11.10 The authorisation should also consider the proportionality of the data to be disclosed to the request filter by the telecommunications operators or postal operators, even if the majority is not expected to be released to the public authority.

11.11 As with other authorisations, the authorising individual 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

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

11.13 The request is sent to the filter which in turn identifies the relevant telecommunications operators or postal operators 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.

11.14 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.

11.15 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 telecommunications operators 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

11.16 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.

11.17 The data owner for any authorised communications data disclosed to the request filter will be the 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.

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

11.19 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.

11.20 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 telecommunications operator or postal operator retention systems which will continue to hold the data for their normal retention period.

11.21 The request filter will only disclose communications data to the person identified in the relevant authorisation, or the authorising individual concerned in accordance with section 69 of the Act.

11.22 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.

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

- providing authorising individuals 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 IPC.

11.24 This information may only be disclosed to:

- authorising individuals 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 IPC for the purposes of the functions of the IPC; or
- when otherwise authorised by law.

11.25 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 telecommunications operators or postal operators 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 set out in chapter 13 regarding data protection.

11.26 Data disclosed to the public authority as a result of use of the request filter must be handled in accordance with chapter 13.

Oversight and reporting

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

11.28 The Secretary of State must consult the IPC about the principles on the basis of which the request filter will be established, maintained or operated.

11.29 The IPC 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 IPC 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 IPC may require changes to be made to the use, operation, or design of the request filter.

11.30 The error reporting provisions detailed in chapter 24 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 IPC 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 24.

12 Technical Capability Notices

12.1 Telecommunications operators or postal operators may be required under section 253 of the Act to have the capability to provide assistance in giving effect interception, equipment interference and bulk acquisition warrants and notices or authorisations for the acquisition of communications data. The purpose of maintaining a technical capability is to ensure that, when a warrant, authorisation or notice is served, companies can give effect to it securely and quickly.

12.2 The Secretary of State may give a relevant telecommunications operator or postal operator a technical capability notice imposing on the relevant operator obligations that are specified in regulations made by the Secretary of State and set out in the notice, and requiring the person to take all steps specified in the notice. The Secretary of State may only give a notice where the decision to do so has been approved by a Judicial Commissioner. In practice, notices will only be given to telecommunications operators and postal operators required to give effect to relevant authorisations (i.e. warrants served under Parts 2, 5 or 6 of the Act, or authorisations and notices given under Part 3 of the Act) on a recurrent basis.

12.3 In the event that a number of telecommunications operators are involved in the provision of a service, the obligation(s) will be placed on the telecommunications operator which is able to give effect to the notice and on whom it is reasonably practicable to impose the requirements. It is possible that more than one telecommunications operator will be involved in the provision of the capability. In such circumstances, it is likely to be necessary for the operator to whom the notice is given to disclose, with the permission of the Secretary of State, the existence of the notice.

12.4 The only obligations that may be imposed by a technical capability notice are those set out in regulations made by the Secretary of State and approved by Parliament. Before making these regulations, the Secretary of State must consult the Technical Advisory Board, telecommunications operators or postal operators appearing to the Secretary of State to be likely to be subject to obligations specified in the regulations, persons representing operators and persons with statutory functions in relation to operators, including the IPC.

12.5 Section 253(4) provides that the obligations that the Secretary of State may include in regulations, and thus which may be imposed on operators, must be reasonable for the purpose of securing that it is (and remains) practicable to impose requirements on a telecommunications operator, and that it is practicable for the operator to comply with those requirements. For example, an obligation relating to the security of a telecommunications service or telecommunication system can be imposed by a technical capability notice for the purpose of ensuring that the operator has the capability to assist in giving effect to an interception warrant in such a manner that the risk of any unauthorised persons becoming aware of the existence of the warrant is minimised. Section 253(5) gives examples of the sorts of obligations that such regulations may include:

- obligations to provide facilities or services of a specified description;
- obligations relating to apparatus owned or operated by a relevant operator;

- obligations relating to the removal of electronic protection applied by or on behalf of the relevant operator on whom the obligation has been placed, to any communications or 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 content or data.

12.6 An obligation imposed by a technical capability notice on a telecommunications operator to remove encryption does not require the operator to remove encryption per se. Rather, it requires that operator to maintain the capability to remove encryption when subsequently served with a warrant, notice or authorisation.

12.7 As with any other obligation contained in a technical capability notice, an obligation to remove encryption may only be imposed where it is reasonably practicable for the relevant telecommunications operator to comply with it. A decision regarding what is reasonably practicable will depend on the particular circumstances of the case, recognising that what is reasonably practicable for one telecommunications operator may not be for another. Such an obligation may only relate to electronic protections that the company has itself applied to communications or data, or where those protections have been applied on behalf of that telecommunications operator, and not to encryption applied by any other party. References to protections applied on behalf of the telecommunications operator or postal operator include circumstances where the telecommunications operator or postal operator has contracted a third party to apply electronic protections to a telecommunications service offered by that telecommunications operator to its customers.

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

Consultation with operators

12.9 Before giving a notice, the Secretary of State must consult the telecommunications operator or postal operator[53]. In practice, informal consultation is likely to take place long before a notice is given in order that the operator understands the requirements that may be imposed and can consider their impact. The Government will engage at an early stage with telecommunications operators or postal operators 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.

12.10 In the event that the giving of a notice to a telecommunications operator or postal operator is deemed appropriate, the Secretary of State must consult the telecommunications operator or postal operator before the notice is given. The Secretary of State may delegate participation in this exercise to their officials. In

[53] See section 255(2).

addition to discussion of the matters listed at para 12.13, the consultation must also include discussion of the design of any technical capability to be used to give effect to authorisations. This will ensure that any capability will meet the requirements of the notice prior to development.

12.11 Should the telecommunications operator or postal operator have concerns about the reasonableness, cost or technical feasibility of the obligations to be set out in the notice, these should be raised during the consultation process. At the conclusion of these discussions, any outstanding concerns must be taken into account by Secretary of State as part of the decision making process.

Matters to be considered by the Secretary of State

12.12 Following the conclusion of consultation with a telecommunications operator or postal operator, the Secretary of State will decide whether to give a notice. This decision should include consideration of all the aspects of the proposed notice and its effect on the telecommunications operator or postal operator. 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.

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

- the likely benefits of the notice – this may take into account projected as well as existing benefits;
- the likely number of users (if known) of any postal or telecommunications service to which the notice relates – this will help the Secretary of State to consider both the necessity of the capability but also the likely benefits;
- the technical feasibility of complying with the notice – taking into account any representations made by the telecommunications operator or postal operator and giving specific consideration to any obligations in the notice to remove electronic protections (as described at section 255(4));
- the likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the telecommunications operator or postal operator as part of the notice, such as those relating to security. This should also include specific consideration to the likely cost of complying with any obligations in the notice to remove electronic protections. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money; and
- any other effect of the notice on the telecommunications operator or postal operator – again taking into account any representations made by the company.

12.14 In addition to the points above, the Secretary of State should consider any other issue which is relevant to the decision. When giving a notice to an operator based in a country outside the UK, this may include consideration of any requirements or restrictions under the law of that country that may arise when the operator complies with any obligation imposed by a technical capability notice, or when the operator provides subsequent assistance in relation to a warrant or other relevant authorisation. Section 2 of the Act also requires the Secretary of State to give

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

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

12.15 When considering the public interest in the integrity and security of telecommunication systems the Secretary of State should consider those systems affected by obligations set out in the notice, with particular reference to any obligations relating to the removal of encryption.

12.16 The Secretary of State may give a notice after considering of the points above if he or she considers that the notice is necessary, and that the conduct required is proportionate to what is sought to be achieved. The obligations set out in the notice must be limited to those set out in regulations made by the Secretary of State under section 253, as described above.

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

Giving a notice

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

12.19 Section 255(6) provides that technical capability notices may be given to, and obligations imposed on telecommunications operators and postal operators 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 telecommunications operator or postal operator[54]:

[54] See section 255(6)

- 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.

12.20 At the time that the notice is given, the person or company to whom a notice is given will be provided with the information they will require to respond to the notice and to subsequent warrants, notices or authorisations.

12.21 As set out in section 253(7), the notice will specify the period within which the telecommunications operator or postal operator 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.

12.22 The notice will also specify the telecommunication services or systems to which the obligations will apply.

12.23 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

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

12.25 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, without the permission of the Secretary of State[55].

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

- to a person (such as a system provider) who is working with the relevant telecommunications operator or postal operator to give effect to the notice;

- to another telecommunications operator whose services or systems are likely to be impacted by the maintenance of the technical capability;

- to relevant oversight bodies;

[55] See section 255(8)

- to a legal adviser for the purposes of advising on compliance or in contemplation of legal proceedings, or for the purpose of those proceedings;
- to regulators in exceptional circumstances where information relating to a capability may be relevant to their enquiries;
- to other telecommunications operators or postal operators subject to a technical capability notice to facilitate consistent implementation of the obligations; and
- in other circumstances notified to and approved in advance by the Secretary of State.

Regular review

12.27 Section 256(2) of the Act imposes an obligation on the Secretary of State to keep technical capability notices under regular review. This helps to ensure that the notice itself, and any of the requirements specified in the notice remain necessary and proportionate. This evaluation differs from the process provided for in section 257 of the Act, which permits telecommunications operators and postal operators to refer a notice back to the Secretary of State for a review.

12.28 It is recognised that, after a notice is given, the telecommunications operator or postal operator 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.

12.29 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.

12.30 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 any element of the notice;
- a significant change in the telecommunications operator's or postal operator's activities or services; or
- a significant refresh or update of the operator's systems.

12.31 When reviewing a technical capability notice, the Secretary of State must consult the telecommunications operator or postal operator in deciding whether the notice remains necessary and proportionate. A review may conclude that the notice should continue to remain in force, be varied to add or remove obligations, or be revoked. The relevant telecommunications operator or postal operator and the operational authorities will be notified of the outcome of the review.

Variation of technical capability notices

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

12.33 Telecommunications operators and postal operators that have been given a technical capability notice may be obliged by regulations to notify the Secretary of State of changes to existing telecommunications services and the development of new services and relevant products in advance of their launch. This will enable the Secretary of State to consider whether it is necessary and proportionate to require the telecommunications operator or postal operator to modify an existing capability or provide a new technical capability on the service.

12.34 Regulations may make an obligation for a technical capability notice to specify the types of changes the Secretary of State considers necessary to be notified. The Secretary of State and a Judicial Commissioner must be content that the level of notification required is necessary and proportionate to what is sought to be achieved, and that it is reasonably practicable to impose this requirement on the relevant operator. As detailed at para 12.9, if the operator has any questions or concerns about any of the obligations in the notice they will have the opportunity to raise these during the consultation process.

12.35 Where a proposed change to an existing telecommunications system or service jeopardises the operator's ability to give effect to an extant notice, the operator must notify the Secretary of State as soon as this is known. Certain changes to services, such as upgrades of systems which are already covered by the existing notice, may be agreed between the Secretary of State and telecommunications operators or postal operators in question where the change would not require new obligations to be imposed on the company. However, significant changes to networks or service which necessitate new obligations being imposed on the company will require a variation of the technical capability notice. The operator must work with the Secretary of State's representatives to make any technical changes required to ensure that the company can meet the requirements of their notice or the notice as varied.

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

12.37 There are a number of reasons why a notice might be varied. These include:

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

12.38 Where a telecommunications operator or postal operator has changed name, for example as part of a rebranding exercise or due to a change of ownership, the

Secretary of State, in consultation with the telecommunications operator or postal operator, must consider whether the existing notice should be varied.

12.39 Before varying a notice, the Secretary of State must consult the telecommunications operator or postal operator to understand the impact of the change and must take into account the same factors as when deciding to give a notice, including cost and technical implications[56]. The Secretary of State or a person operating on their behalf should also consult public authorities to understand the operational impact of any change to the notice.

12.40 Further detail on the consultation process and matters to be considered by the Secretary of State can be found above at paragraphs 12.9-12.16.

12.41 Once a variation has been agreed by the Secretary of State, and the decision to vary a notice has (where necessary) been approved by a Judicial Commissioner, arrangements will be made for the telecommunications operator or postal operator to receive notification of this variation and details of the timeframe in which steps specified in the notice as varied should be taken by the telecommunications operator or postal operator. 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

12.42 A technical capability notice must be revoked (in whole or in part) if it is no longer necessary to require a telecommunications operator or postal operator to provide a technical capability or if it is no longer reasonable to impose certain obligations on the provider.

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

12.44 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 telecommunications operator or postal operator in the future should it be considered necessary and proportionate to do so.

[56] See section 255(3)

13 General safeguards

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

13.2 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. Such data as is held should be adequate, relevant and not excessive in relation to the purpose.

13.3 In addition, the requirements of the relevant data protection legislation must be adhered to.

13.4 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[57]. 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.

13.5 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 53 of the Act.

13.6 Communications data acquired under the Act and all copies, extracts and summaries of it, 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 relevant data protection legislation. Data must be effectively protected against unauthorised access and use, with particular consideration given to the principles of data security and integrity.

13.7 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.

13.8 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

[57] 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.

occasions where it is necessary for a public authority to disclose data to an overseas authority.

13.9 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. Subject to the exceptions set out in paragraphs 13.32-13.36 (disclosure of communications data to overseas authorities) 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.

13.10 Communications 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 copies of relevant data held by the public authority 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.

13.11 If such material is retained, it should be reviewed when appropriate to confirm that the justification for its retention is still valid for one or more of the authorised purposes.

13.12 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 data protection 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.

13.13 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 that the resultant combined data is subject to the highest possible security standard applicable.

Disclosure of communications data and subject access rights

13.14 This section of the code provides guidance on the relationship between disclosure of communications data under the Act, telecommunications operators' or postal operators' obligations to comply with a notice to disclose data, and individuals' right of access under relevant data protection legislation to personal data held about them.

13.15 The right of a person to seek personal data held about them is not overridden by the offence at section 82 of the Act. Where such a request is made, a telecommunications operator or postal operator may rely on certain exemptions to the right of subject access specified in data protection legislation[58].

13.16 Data will always be exempt from disclosure where such an exemption is required for the purposes of safeguarding national security.

---

[58] There may be other bars to disclosure in other legislation, for example regarding impeding a criminal investigation.

13.17 Personal data processed for the purposes of the prevention and detection of crime, the apprehension or prosecution of offenders or another imposition of a similar nature are also exempt to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters.

13.18 The exemption to subject access rights does not automatically apply. In the event that a telecommunications operator or postal operator receives a subject access request where the fact of a disclosure under the Act might itself be disclosed, the telecommunications operator or postal operator 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.

13.19 Where a telecommunications operator or postal operator 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 must provide a response which will enable the telecommunications operator or postal operator to comply with its obligations to respond to the subject access request within 40 days at the latest. 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 set out in paragraph 13.17. If the public authority does not want the fact of the notice to be disclosed to the subject then they must provide the telecommunications operator or postal operator with sufficient justification as to the exemptions.

13.20 Where a telecommunications operator or postal operator withholds a piece of information under exemptions in relevant data protection legislation, 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.

13.21 Telecommunications operators and postal operators 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 data protection legislation, an individual may request that the Information Commissioner assesses whether a subject access request has been handled in compliance with such legislation.

Acquisition of communication data on behalf of overseas authorities

13.22 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.

13.23 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.

13.24 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

13.25 A central authority in the United Kingdom may receive a request for mutual legal assistance (MLA) including by way of a European Investigation Order, 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.

13.26 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, unless it is in the form of a European Investigation Order where the process is set out below, may then be considered and, if appropriate, executed by that public authority under Part 3 of the Act and in line with the guidance in this code of practice.

13.27 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.

European Investigation Orders

13.28 Where a request is made in the form of a European Investigation Order, a judicial authority in the Member State requesting assistance will already have decided that it is necessary and proportionate to obtain the information sought for the purposes of a criminal investigation or proceedings. The principle of mutual recognition applies, and assistance may only be refused if one or more of the grounds for refusal set out in the Directive, and transposed into national law in regulation 28 of, and Schedule 4 to, the Criminal Justice (European Investigation Order) Regulations 2017, applies.

13.29 A European Investigation Order will never need to be authorised under Part 3 of the Act because the UK will accept the authorisation that has taken place in the requesting Member State. However, where the assistance of a relevant public authority is sought in acquiring communications data the relevant public authority will need to ensure the request is not inconsistent with requirements in UK legislation. If there are concerns about necessity and proportionality the relevant public authority may request the UK central authority which received the request

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

revert to the authority responsible for issuing the European Investigation Order for further information.

Non-judicial co-operation

13.30 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.

13.31 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.

Disclosure of communications data to overseas authorities

13.32 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 protection. Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

13.33 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.

13.34 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].

13.35 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, and, if necessary, the Commissioner's office can provide guidance.

13.36 Data protection legislation 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'. 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.

---

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

That is a decision that can only be taken by the public authority holding the data on a case by case basis.

14 Notification

14.1 This section provides information regarding circumstances in which an individual may be notified about the acquisition of their communications data under Part 3 of the Act.

Duty to consider notification

14.2 Where communications data is being sought from a telecommunications operator or postal operator, if the telecommunications operator or postal operator is permitted to notify the subject(s) of the fact that a request has been made for their data the relevant public authority must specify this when requesting the data. The public authority must, at the point of application, consider whether it would be damaging to investigations to notify the individual that their data will be acquired.

14.3 Where it would not be damaging to investigations, the public authority may allow the telecommunications operator or postal operator to notify the individual, for example when the telecommunications operator or postal operator receives a subject access request under data protection legislation. Where it would be damaging to investigations the public authority must make clear that the telecommunications operator is not to notify the subject.

Notification of serious errors under the Act

14.4 As identified in chapter 24 of this code, there may be rare occasions when communications data is wrongly acquired or disclosed. In these cases, the public authority which made the error, or established that the error had been made, must report the error to the authority's senior responsible officer and the Investigatory Powers Commissioner (IPC). In accordance with section 231 of the Act, when an error is reported to the IPC, the IPC may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal.

14.5 In considering whether to notify an individual of an error, the IPC must be satisfied that the error is a) a serious error and b) it is in the public interest for the individual concerned to be informed of the error (see section on serious errors beginning at paragraph 24.33).

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

Notification in criminal proceedings

14.7 Where communications data has been acquired during the course of a criminal investigation that comes to trial an individual will be made aware, in most cases, that data has been obtained.

14.8 Where communications data is used to support the prosecution case it will be served as evidence on the defendant. Additionally in compliance with its disclosure obligations pursuant to the Criminal Procedure and Investigations Act 1996 (CPIA), the prosecution will reveal the existence of communications data (and potentially the material generated in the process of it being obtained) to a defendant on a schedule of non-sensitive unused material, if that data is relevant[61]. Such material will be provided to the defendant if, pursuant to section 3 of the CPIA, such material is reasonably considered capable of undermining the prosecution case and/or assisting the defence case.

14.9 The CPIA sets out exemptions to the disclosure obligation. Under section 3(6) of that Act, data must not be disclosed if it is material which, on application by the prosecutor, the Court concludes it is not in the public interest to disclose. Any communications data which comes within the scope of this exemption cannot be disclosed to the accused.

14.10 If through any of the above notification processes, an individual suspects that their communications data has been wrongly acquired, the Investigatory Powers Tribunal provides a right of redress. As set out further in chapter 26.3, an individual may make a complaint to the Tribunal, without the individual knowing, or having to demonstrate that any investigatory powers have been used against them.

[61] Data may be relevant if it has some bearings on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case.

15 Compliance and offences

15.1 The Act places a requirement on telecommunications operators and postal operators to comply with a requirement imposed on them by a notice under Part 3 of the Act. Telecommunications operators and postal operators are not however required to take any steps which it is not reasonably practicable for them to take.

15.2 What is reasonably practicable will be considered on a case-by-case basis, taking into account the individual circumstances of the relevant telecommunications operator or postal operator. 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.

15.3 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 an obligation under Part 3 of the Act.

15.4 When considering whether it is reasonably practicable for a person outside the UK to comply with a notice, section 85(4)(a) specifies that regard must be had to any requirements or restrictions under the law of the country where the telecommunications operator or postal operator is based that are relevant to the taking of those steps. It also makes clear the expectation that telecommunications operators and postal operators 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 telecommunications operator or postal operator 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.

15.5 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

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

Acquisition Offence

15.7 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.

15.8 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 mitigate the risk of any offence being committed.

15.9 The offence is not committed if the person who obtained the communications data can show that they acted in the reasonable belief that they had lawful authority to obtain the data.

15.10 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 telecommunications operator or postal operator despite the fact that they could not have genuinely believed that an authorisation would be in place.

15.11 In particular, it is not an offence to obtain communications data where it is made publicly or commercially available by the telecommunications operator or postal operator or otherwise where the telecommunications operator or postal operator freely consents to its disclosure. In such circumstances the consent of the operator provides the lawful authority for the obtaining of the data. However, as set out above, relevant public authorities should not require, or invite, any postal or telecommunications operator to disclose communications data by relying on any exemption to restrictions on disclosing personal data under relevant data protection legislation

Disclosure offence

15.12 Under section 82, it is an offence for a telecommunications operator to disclose without reasonable excuse the existence of an authorisation or notice for communications data by a public authority under the Act.

15.13 The offence of unauthorised disclosure occurs when any telecommunications operator or postal operator, or employee of a telecommunications operator or postal operator, reveals the existence of a requirement to disclose communications data about a particular person to that person.

15.14 It is a reasonable excuse for a telecommunications operator or postal operator to disclose such information when the public authority making the authorisation gives permission to do so. A public authority must consider for each acquisition of communications data whether to give permission to the telecommunications operator or postal operator to disclose the authorisation for communications data. If permission is given, the public authority must specify to the telecommunications operator or postal operator the circumstances under which disclosure may take place.

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

15.16 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 61(7) of the Act.

15.17 Circumstances in which it may be appropriate to give permission to disclose the existence of a specific authorisation or notice for communications data may include where communications data is required to be disclosed to assist in the investigation of a crime of which the subject of the authorisation or notice 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. However, this will always depend on the specific circumstances of the investigation.

15.18 It is very unlikely to be a reasonable excuse for a telecommunications operator or postal operator to disclose such information in the interests of transparency to its customers without the permission of the relevant public authority.

Section 3

Communications data retention

16 General extent of powers

Necessity and proportionality

16.1 Section 87(1) of the Act gives the Secretary of State the power to give a data retention notice to a telecommunications operator or postal operator, requiring them to retain relevant communications data, if it is considered necessary and proportionate for one or more statutory purposes. These are:

- in the interests of national security;
- for the applicable crime purpose[62];
- 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 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; and
- 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.

16.2 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 the notice could reasonably be achieved by other less intrusive means,
- whether the level of protection to be applied in relation to obtaining communications data is higher because of the particular sensitivity of that information,
- 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.

16.3 Data retained for the purposes set out above can only be accessed by public authorities for those purposes under Part 3 of the Act, where it is necessary and proportionate to do so or under other appropriate statutory regimes. 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.

---

[62] To the extent that a retention notice relates to events data this is the purpose of preventing or detecting serious crime. To the extent that a retention notice relates to entity data this is the purpose of preventing or detecting crime or of preventing disorder (see paragraph 3.4)

17 Giving of data retention notices

Process for giving a data retention notice

17.1 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 give a data retention notice.

17.2 Once a potential requirement is identified, the Home Office will consult the relevant telecommunications operator(s) or postal operator(s) and, if appropriate, the Secretary of State will consider giving a notice.

Criteria for issuing a data retention notice

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

- the size of the telecommunications operator or postal operator – an operator with a larger customer base is more likely to receive a data retention notice;
- the speed of growth of the telecommunications operator or postal operator – small telecommunications operators or postal operators with rapid prospective growth may receive notices in anticipation of future law enforcement requirements;
- the number of authorisations or notices the telecommunications operator or postal operator receives annually for communications data – this, and the operator's ability to meet the volume of authorisations or notices they receive, will be a key determinant of whether there is benefit in giving a notice to a telecommunications operator or postal operator (noting that the giving of a notice may increase the number of authorisation or notices received by an operator);
- whether the telecommunications operator or postal operator operates a niche service – an operator 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 the telecommunications operator or postal operator operates in a specific geographical area – an operator which is a key provider of services in a limited geographical area is more likely to receive a notice.

17.4 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 and where the decision to do so has been approved by a Judicial Commissioner.

17.5 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.

17.6 Where a telecommunications operator 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 or can best access 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.

17.7 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 the subject of two retention notices.

Criteria for giving a notice to categories of providers

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

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

17.10 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

17.11 Before giving a notice to a company the Secretary of State must take reasonable steps to consult any telecommunications operator(s) or postal operator(s) which will be subject to the notice.

17.12 In practice, informal consultation is likely to take place long before a notice is given in order that the operator(s) understands the requirements that may be imposed and can consider the impact. The Government will engage at an early state with telecommunications operators or postal operators who may be subject to a notice in the future to provide advice and guidance and prepare them for the possibility of receiving a notice.

17.13 In the event that the giving of a notice to a telecommunications operator or postal operator is deemed appropriate, the Secretary of State must take reasonable steps to consult the company before giving a notice, in order to ensure that it accurately reflects the services and data types processed by that telecommunications operator or postal operator and to ensure that the telecommunications operator or postal operator understands the obligations being placed on it, including those in relation to the audit functions of the Information Commissioner. The Secretary of State may delegate participation in this exercise to their officials. In addition to discussion of the matters listed at paragraph 17.17, the consultation must also include discussion of the design of any systems to be put in place to give effect to the requirements of the notice.

17.14 Should the telecommunications operator or postal operator have concerns about whether the reasonableness, cost or technical feasibility of the requirements to be set out in the notice, these should be raised during this consultation process. At the conclusion of these discussions, any outstanding concerns must be taken into account by the Secretary of State as part of the decision making process. Should a telecommunications operator or postal operator continue to have concerns in respect of the feasibility of a notice once given they may refer the notice for review (see chapter 23).

17.15 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 telecommunications operators or postal operators 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 telecommunications operator or postal operator enters the market after a notice has been given and therefore will not have been formally consulted. In such circumstances the Secretary of State must take reasonable steps to consult any relevant telecommunications operators and postal operators which enter the market after such a notice is given.

Matters to be considered by the Secretary of State

17.16 Following the conclusion of consultation with a telecommunications operator or postal operator, the Secretary of State will consider whether to give a data retention notice. This decision should include consideration of all the aspects of the proposed data retention notice and its effect on the telecommunications operator or postal operator. It is an essential means of ensuring that the data retention notice is justified and that proper processes have been followed.

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

- the likely benefits of the notice in respect of each of the services to which it relates, including 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 and must be in respect of the statutory purposes for which the data can be retained;
- the appropriateness of limiting data to be retained by reference to location or descriptions of persons to whom telecommunications services are provided. These considerations will include determining whether the full geographical reach of the retention notice is necessary and proportionate and whether it is necessary and proportionate to include or exclude any particular descriptions of persons.
- the likely number of users (if known) 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 to be retained;
- the technical feasibility of complying with the notice – taking into account any representations made by the telecommunications operator(s) or postal operator(s)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 telecommunications operators or postal operators, 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 effect of the notice on the telecommunications operator or postal operator – again taking into account any representations made by the company.

17.18 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[64].

17.19 In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision. When giving a notice to an operator based in a country outside the UK, this may include consideration of any requirements or restrictions under the law of that country that may arise when the operator complies with any obligation imposed by a data retention notice. Section 2 of the Act also requires the Secretary of State to give regard to the following when giving, varying or revoking a notice so far as they are relevant:

- whether what is sought to be achieved by 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.

17.20 When considering the public interest in the integrity and security of telecommunication systems the Secretary of State should consider those systems affected by obligations set out in the notice.

17.21 The Secretary of State may give a notice after considering of the points above if he or she considers that the notice is necessary, and that the conduct required is proportionate to what is sought to be achieved.

Judicial Commissioner Approval

17.22 Before a data retention notice can be given, the Secretary of State's decision to give it must be approved by a Judicial Commissioner. In deciding whether to approve the Secretary of State's decision to give a retention notice, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the notice is necessary and whether the conduct it requires is proportionate to what is sought to be achieved. In reviewing these conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. The Judicial Commissioner must review the conclusions with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed

---

63 See paragraph 17.17 for details of the matters the Secretary of State will consider before issuing a data retention notice.

64 See paragraphs 17.35-17.42 for further information on retention periods.

by section 2 (general duties in relation to privacy).If the Judicial Commissioner refuses to approve the decision to give the notice the Secretary of State may either:

- not give the notice; or,
- refer the matter to the Investigatory Powers Commissioner for a decision (unless the they have made the original decision).

17.23 If the IPC refuses the decision to give the notice the Secretary of State must not give the notice. There is no further avenue of appeal available.

17.24 The Act does not mandate how the Judicial Commissioner must show or record their decision. These practical arrangements should be agreed between the Secretary of State and the IPC. The Act does not, for example, require the Judicial Commissioner to sign a legal instrument. This means that a Judicial Commissioner can provide oral approval to give a notice. It is important that a written record is taken of any such approvals.

Giving a notice

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

17.26 Section 97 provides that a data retention notice may be given to, and impose obligations on telecommunications operators and postal operators located outside the UK and may require things to be done outside the UK.

17.27 A data retention notice comes into force from the point it is given to the telecommunications operator or postal operator, unless otherwise specified in the notice.

17.28 It will often be the case that dedicated systems will be constructed within a telecommunications operator or postal operator 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.

17.29 Once a notice has been given to a telecommunications operator or postal operator, 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 25 for further details).

The content of a data retention notice

17.30 A notice will set out:

- the telecommunications operator(s) or postal operator(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;
- the services in relation to which data is to be retained – for example, it may not be necessary and proportionate to retain data in relation to all communications 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 87(11) of the Act and will make clear how long certain categories of data should be retained for[65]; 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 telecommunications operator's or postal operator's compliance with these requirements by the Information Commissioner.

17.31 A notice will not necessarily represent the full range of services and data types which a telecommunications operator or postal operator could retain. This does not mean that additional data types or services could not be included in a future version of the notice, should an operational requirement arise, provided that it would be necessary and proportionate to do so (see chapter 18 for further details).

17.32 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 telecommunications operator or postal operator (including transitory information in the core systems) is made available to be retained;
- a requirement to process the data to ensure that multiple items of data from a single system or multiple systems within an operator 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; or
- a requirement to test the viability of retaining certain data or developing a retention system over a phased timescale.

Generation & processing of data

17.33 A retention notice may also include requirements in relation to the generation and processing of retained 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 authorisations and notices (including linking events to user accounts);

[65] The data to be retained must be covered in sufficient detail that the telecommunications operator or postal operator is clear exactly what it must retain.

- a requirement to take such steps as are necessary to ensure that data which is generated and processed by the telecommunications operator or postal operator 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 systems within an operator 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;

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

Retention period

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

17.36 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.

17.37 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.

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

17.39 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.

17.40 For retained data held by a telecommunications operator or postal operator 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 a maximum of 12 months after the telecommunications operator or postal operator changes the data in their systems, irrespective of whether the customer remains with the service.

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

17.42 Sometimes a telecommunications operator or postal operator 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 telecommunications operator or postal operator decides to delete the data.

18 Review, variation and revocation of retention notices

Regular review

18.1 Section 90(13) of the Act imposes an obligation on the Secretary of State to keep data retention notices under regular review. This helps to ensure that the notice itself, and any of the requirements specified in a notice, remains necessary and proportionate. This evaluation differs from the process provided for in in the rest of Section 90 of the Act, which permits telecommunications operators and postal operators to refer a notice back to the Secretary of State for a review (see chapter 23 for further details).

18.2 It is recognised that, after a notice is given, a telecommunications operator or postal operator is likely to require time to put the necessary capabilities in place to meet their obligations. 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.

18.3 A review of a data retention 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.

18.4 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 any element of the notice;
- a significant change in the telecommunications operator's or postal operator's activities or services;
- a significant refresh or update of the operator's systems; or
- where the notice contains a certain date by which the telecommunications operator or postal operator must comply with the requirement. In such circumstances an early review might be appropriate to determine the telecommunications operator or postal operator is on course to meet that requirement.

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

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

18.7 Once this process is complete, the Secretary of State will consider whether the notice remains necessary and proportionate. A review may conclude that the notice should continue to remain in force, be varied to add or remove obligations, or be revoked. The relevant telecommunications operator or postal operator, the operational agencies and the Information Commissioner will be notified of the outcome of the review.

Variation

18.8 The communications market is constantly evolving and telecommunications operators or postal operators subject to data retention notices will often launch new services or generate new data that relevant public authorities may require.

18.9 Telecommunications operators and postal operators subject to a data retention notice must notify the Secretary of State of changes to existing telecommunications or postal services covered by the notice and any other products they consider may be relevant as soon as possible. This will enable the Secretary of State to consider whether it is necessary and proportionate to require data generated or processed in the course of providing those services to be retained.

18.10 Certain changes to services, such as upgrades of systems or changes to data which are already covered by the existing notice, may be agreed between the Secretary of State and the telecommunications operator or postal operator in question where the change would not require new obligations to be imposed on the company. However, significant changes to networks or service which necessitate new obligations being imposed on the company will require a variation of the data retention notice. The operator must work with the Secretary of State's representatives to make any technical changes required to ensure that the company can meet the requirements of their notice or the notice as varied.

18.11 Section 94 of the Act provides that data retention notices can be varied by the Secretary of State if the Secretary of State considers that the variation is necessary and the conduct required by the variation is proportionate to what is sought to be achieved. Where the variation requires the retention of additional communications data, the decision to vary a notice must be approved by a Judicial Commissioner. Judicial Commissioner approval is not required where a variation does not require the retention of additional data.

18.12 There are a number of reasons a notice might be varied. These include:

- a telecommunications operator or postal operator launching new services or generating new categories of communications data which may be of interest to law enforcement;
- changing law enforcement demands and priorities, including removing a requirement to retain data when no longer necessary and proportionate;
- 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.

18.13 Where a telecommunications operator or postal operator has changed name, for example as part of a rebranding exercise or due to a change of ownership, the

Secretary of State, in consultation with the telecommunications operator or postal operator, must consider whether the existing notice should be varied.

18.14 Before varying a notice, the Secretary of State must consult the telecommunications operator or postal operator to understand the impact of the change and must take into account the same factors as when deciding to give a notice, including cost and technical implications. The Secretary of State or a person acting on their behalf should also consult public authorities to understand the operational impact of any change to the notice.

18.15 Further detail on consultation process and matters to be considered by the Secretary of State can be found in chapter 17.

18.16 Once a variation has been agreed by the Secretary of State and, where the notice includes the retention of additional data, approved by a Judicial Commissioner, arrangements will be made for the telecommunications operator or postal operator to receive notice of this variation and details of the timeframe in which steps specified in the notice as varied should be taken by the telecommunications operator or postal operator. 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. .

18.17 Once a variation notice has been given to a telecommunications operator or postal operator a copy will be sent to the Information Commissioner.

18.18 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

18.19 A data retention notice must be revoked (in whole or in part) if it is no longer necessary to require the relevant telecommunications operator or postal operator to retain communications data, or certain types of communications data.

18.20 Circumstances in which it may be appropriate to revoke a notice include where a telecommunications operator or postal operator 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.

18.21 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 telecommunications operator or postal operator in the future should it be considered necessary and proportionate to do so.

18.22 Once notice of revocation has been given to a telecommunications operator or postal operator a copy will be sent to the Information Commissioner.

19 Security, integrity and destruction of retained data

19.1 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 92 of the Act requires telecommunications operators and postal operators 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.

19.2 Further detail on the security arrangements to be put in place by telecommunications operators and postal operators may be included in the data retention notice given to a telecommunications operator or postal operator which, in accordance with section 87(8)(d), must specify any other requirements or restriction in relation to the retention of data.

19.3 In most cases data retained under a notice is stored in a dedicated data retention system, which is securely separated by technical security measures (e.g. a firewall) from a telecommunications operator's or postal operator's business system. Where data is retained by telecommunications operators or postal operators for business purposes for some, but not all, of the period specified in the notice, the data retention system may hold a duplicate of that business data so that it can be accessed efficiently and effectively[66].

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

19.5 The scope of the security controls defined within this section apply to all systems where data is retained by virtue of a retention notice. The security controls also include any other systems which are used to access, support or manage data retained under a retention notice. The security controls also apply to all telecommunications operator or postal operator (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.

19.6 Where data is retained in business or shared systems, or where business systems are used to access, support or manage systems containing data retained by virtue of a retention notice, 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.

19.7 Where data was originally retained by virtue of a retention notice but it has subsequently been moved or copied by the telecommunications operator or postal operator into another system, the security controls in the Act and this code do not apply. This is because the scope of these security controls can only apply insofar as

---

66 See paragraph 17.2

they relate to data retained by virtue of a retention notice. However, any processes or systems that are involved in the transferring or copying of data retained under a retention notice into another system are subject to these security controls.

Data security

19.8 The specific data security measures required by a telecommunications operator or postal operator 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.

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

19.10 The security put in place at a telecommunications operator or postal operator 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.

19.11 As each of these broad areas is complementary, the balance between these may vary e.g. a telecommunications operator or postal operator 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 telecommunications operators or postal operators and shared with the Information Commissioner for the purposes of his functions under this code.

19.12 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 telecommunications operators and postal operators retaining data will be required to follow the key principles of data security set out in paragraphs 19.19 to 19.42. It is open to a telecommunications operator or postal operator to put in place alternative controls or mitigations which provide assurance of the security of the data where agreed with the Home Office.

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

Data integrity

19.14 Data integrity, as required by section 92(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 altered[67].

19.15 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 telecommunications operator or postal operator in understanding network loading may be less accurate than data used to bill customers.

19.16 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.

19.17 Once the data has been retained, technical security controls should 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 92(2) of the Act.

19.18 The audit capability of the data retention system should 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

19.19 All data retention and disclosure systems and practices must be compliant with relevant legislation. As well as the Act, this includes relevant data protection legislation, which sets out key controls in relation to the storage, use and transfer of personal data.

19.20 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 published guidance on security. Further requirements are unlikely to be publicly available where they contain specific details of security infrastructure or practices, disclosure of which could create additional security risks.

Information security policy & risk management

19.21 Each telecommunications operator or postal operator must develop a security policy document. The policy document should describe the internal security organisation, the governance and authorisation processes, access controls, necessary training,

---

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

the allocation of security responsibilities and policies relating to the integrity and destruction of data. Each telecommunications operator or postal operator must also develop security operating procedures, including clear desk and screen policies for all systems. A telecommunications operator or postal operator can determine whether this forms part of or is additional to wider company policies.

19.22 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.

19.23 Each telecommunications operator or postal operator must identify, assess and treat all information security risks, including those which relate to arrangements with external parties.

Human Resources security

19.24 Telecommunications operators and postal operators 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.

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

Maintenance of physical security

19.26 Data retention 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.

19.27 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 19.43).

Operations management

19.28 Data retention 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.

19.29 Telecommunications operators and postal operators must also put in place a patching policy to ensure that regular patches and updates are applied to any data retention 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.

19.30 Telecommunications operators and postal operators should ensure that, where encryption is in place in data retention systems, any encryption keys are subject to appropriate controls, in accordance with the security policy.

19.31 In order to maintain the integrity of internal data processing telecommunications operators and postal operators must ensure that data being processed is validated against agreed data security criteria.

19.32 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.

19.33 Telecommunications operators and postal operators 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.

19.34 The data retention system, and its use, should be monitored and all audit logs compiled, secured and reviewed by the telecommunications operator's or postal operator's security manager at appropriate intervals. These should be made available for inspection by the Home Office as required.

19.35 Telecommunications operators and postal operators should ensure that systems are resilient to failure and data loss by creating regular back-ups of the data.

19.36 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

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

19.38 Access to operating systems must be locked down to an appropriate standard and any mobile computing (i.e. offsite access to telecommunications operator or postal operator 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.

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

Management of incidents

19.40 Telecommunications operators and postal operators 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, should be notified in accordance with those provisions.

19.41 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.

19.42 System managers must ensure that data retention 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

19.43 Section 92(2) of the Act makes clear that retained data must be destroyed[68] 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.

19.44 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 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).

19.45 Where the implemented security measures are assessed by the Home Office, or Information Commissioner, to be insufficient to protect the data retention 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

19.46 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.

19.47 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.

19.48 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.

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

Location of retained data

19.50 The location of retained data will be relevant to the security of the data, however ensuring the data is retained securely is more important than a general requirement on where the data must be retained that does not take account of specific circumstances.

---

[68] Section 263(1) of the Act 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.'

19.51 On that basis, communications data that is subject to a data retention notice and is generated and processed in the European Union must be retained in the European Union unless specific criteria are met. The data can only be transferred and retained outside the European Union where:

1) It is consistent with European Union data protection requirements to transfer the data; and
2) It is deemed that the data can be retained at least as securely outside the European Union

19.52 Where communications data that is subject to a data retention notice is generated and processed outside the European Union a decision will need to be taken on whether the data should be transferred into the European Union. Such a transfer should only take place where:

1) It is consistent with European Union data protection requirements to transfer the data; and
2) It is agreed that the benefits of retaining the data in the EU outweigh the risks to security created by the transfer of the data.

19.53 Once the United Kingdom is no longer a member of the European Union these requirements will not apply as they do while the United Kingdom is a member. However, the principles of only transferring data when it is consistent with data protection requirements and ensuring the data is retained to an appropriate level of security will apply.

20 Disclosure and use of data

Disclosure of data

20.1 As per section 92 of the Act, a telecommunications operator or postal operator 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.

20.2 Section 87(9)(a) of the Act clarifies that telecommunications operators and postal operators can be required to retain data in such a way that it can be transmitted efficiently and effectively in response to requests for communications data. In such circumstances, the Home Office will work with telecommunications operators and postal operators to ensure that the necessary secure auditable systems are in place to enable this disclosure[69].

20.3 The main purpose of retaining relevant communications data is to make that data available, where necessary and proportionate, for disclosure under Part 3 of the Act. However, there may be other circumstances in which telecommunications operators and postal operators may lawfully disclose retained communications data. Such circumstances could include:

- if an emergency service requests data in relation to an emergency call (chapter 10);
- requests for personal data held by a company via a subject access request under relevant data protection legislation[70];
- where a telecommunications operator or postal operator proactively discloses communications data to relevant public authorities or regulatory bodies such as in cases of suspected criminality.

Use of data by telecommunications operators and postal operators

20.4 If data is held subject to a notice and would not otherwise be held by the telecommunications operator or postal operator for business purposes, it should be adequately safeguarded to ensure that it can only be accessed for purposes connected to that notice. If data is not also being retained for existing business purposes it cannot be used by telecommunications operators and postal operators for business purposes without permission from the Home Office. Home Office permission would not be given for matters such as marketing. However, there may be some circumstances where it could be considered in the public interest for the telecommunications operator or postal operator to access the retained data. For

[69] Requiring telecommunications or postal operators to retain communications data in such a way that the data can be transmitted efficiently and effectively in response to requests may include specifying expected response times to requests.

[70] See paragraph 13.14.

example, if a customer is receiving malicious calls or if a telecommunications operator or postal operator identifies suspected criminality on the network. Home Office agreement for the telecommunications operator or postal operator to access the retained data in such circumstances may relate to individual requests or categories of request.

21 Compliance

21.1 The Act places a requirement on telecommunications operators and postal operators to comply with a requirement or restriction imposed on them by a retention notice or otherwise 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 brought 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.

Disclosure of a retention notice

21.2 The Home Office does not publish or release identities of telecommunications operators and postal operators subject to a data retention notice as to do so may identify operational capabilities or harm the commercial interests of companies that have been given a notice. Should criminals become aware of the capabilities of law enforcement then, they may alter their behaviours and switch operator making it more difficult to detect their activities of concern.

21.3 Section 95(2) of the Act prohibits a telecommunications operator or postal operator or an employee of the operator 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. That duty is enforceable by civil proceedings brought by the Secretary of State.

21.4 Section 95(4) provides that the prohibition on a disclosure does not apply if the existence or contents of a data retention notice is disclosed with the permission of the Secretary of State. For example, permission is likely to be given in circumstances including disclosure:

- to a person (such as a system provider) who is working with the relevant telecommunications operator or postal operator to give effect to the notice;
- to another telecommunications operator or postal whose services or systems are likely to be impacted by the retention of data;
- to relevant oversight bodies;
- to a legal adviser in contemplation of legal proceedings, or for the purpose of those proceedings;
- to regulators in exceptional circumstances where information relating to a retention notice may be relevant to their enquiries;
- to other telecommunications operators or postal operators subject to a retention notice to facilitate consistent implementation of the obligations; and
- in other circumstances notified to and approved by the Secretary of State.

Section 4

General matters

22 Costs

Making of contributions

22.1 Section 249 of the Act recognises that telecommunications operators and postal operators incur expenses in complying with requirements in the Act, including the disclosure of communications data in response to authorisations or notices under Part 3 of the Act and the retention of communications data under Part 4. The Act, therefore, allows for appropriate payments to be made to them to cover these costs.

22.2 The following sections outline the circumstances where the Government will make contributions towards the costs of complying with Parts 3 and 4 of the Act. Telecommunications operators and postal operators who are required to retain communications data will inevitably be required to disclose communications data in response to lawful authorisations or notices. In those circumstances the Government will make contributions towards the costs of both retaining and disclosing the data. However, most telecommunications operators and postal operators that are required to disclose data are unlikely to be the subject of a data retention notice. In those circumstances they will only be asked to disclose data that they retain for business purposes. For such telecommunications operators and postal operators, the Government will only make contributions towards the costs of disclosing the data in response to authorisations under Part 3 of the Act.

Contributions of costs for the acquisition and disclosure of communications data

22.3 Significant public funding is made available to telecommunications operators and postal operators 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.

22.4 An effective and efficient response requires the timely disclosure of communications data. In this code 'timely disclosure' means that ordinarily a telecommunications operator or postal operator should disclose data within agreed service levels[71] or, where there are no agreed service levels within ten working days of being required to do so.

22.5 It is legitimate for a telecommunications operator or postal operator to seek contributions towards its costs which may include funding of those general business overheads required in order to facilitate the timely disclosure of communications data.

[71] Defined service levels may be agreed between the Secretary of State and telecommunications operator or postal operator, for example where a retention notice includes requirements to provide for data to be transmitted efficiently and effectively in response to requests. Such service levels may be specified in the notice.

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

22.7 Contributions may also be appropriate towards costs incurred by a telecommunications operator or postal operator 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.

22.8 Where a telecommunications operator or postal operator identifies that an authorisation or notice 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 authorisation or notice is reasonably practicable.

Costs in relation to a technical capability notice

22.9 Telecommunications operators and postal operators 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.

22.10 Any contribution towards these costs must be agreed by the Secretary of State before work is commenced to develop, install or operate the capability. Furthermore, the Secretary of State must be satisfied that the proposed capability will meet the requirements set out in the notice.

22.11 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 telecommunications operators or postal operators in complying with their obligations outlined above. This is particularly relevant for telecommunications operators and postal operators that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems. Further guidance with respect to cost recovery will be made available to all telecommunications operator and postal operators who maintain a technical capability.

Contributions of costs for the retention of communications data

22.12 The above considerations may be appropriate for all telecommunications operators or postal operators that are required to disclose data. The following considerations only apply to those telecommunications operators or postal operators 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.

22.13 Any contribution towards these costs must be agreed by the Home Office before work is commenced by a telecommunications operator or postal operator and will be subject to the Home Office considering, and agreeing, the solution proposed by the telecommunications operator or postal operator.

22.14 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 telecommunications operators or postal operators in complying with their obligations outlined above. Costs may also include costs related to feasibility studies conducted during the period in which a telecommunications operator or postal operator is being consulted prior to a retention notice being given.

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

22.16 Contributions may also be appropriate towards the costs incurred by a telecommunications operator or postal operator 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.

22.17 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

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

22.19 As costs are reimbursed from public funds, telecommunications operators and postal operators should take into account value for money when procuring, operating and maintaining the infrastructure required to comply with a notice. As changes to the operator's business may necessitate changes to data retention systems and technical capabilities, telecommunications operators and postal operators should take this into account when altering business systems and should notify the Secretary of State of proposed changes.

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

Power to develop compliance systems

22.21 In certain circumstances it may be more economical for products to be developed centrally, rather than telecommunications operators, postal operators 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).

22.22 Section 250 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop consistent systems to be used by telecommunications operators and/or postal operators to retain or disclose communications data or systems to be used by public authorities to acquire communications data. Such systems can operate in respect of multiple powers under the Act

22.23 Where such systems are developed for use in telecommunications operators and/or postal operators the Secretary of State will work closely with such operators to ensure the systems can be properly integrated into their networks.

23 Referral of technical capability and data retention notices

23.1 The Act includes clear provisions for telecommunications operator or postal operator to request a review of the requirements placed on them in a technical capability notice or data retention notice should they wish to do so. A person may refer the whole or any part of a notice back to the Secretary of State for review under the Act.

23.2 The circumstances and timeframe within which a telecommunications operator or postal operator 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 telecommunications operator or postal operator 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 given.

23.3 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 TAB must consider the technical requirements and the financial consequences of the notice for the person who has made the referral. The Judicial Commissioner will consider whether the notice is proportionate.

23.4 The Judicial Commissioner and the TAB must give the relevant telecommunications operator or postal operator 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.

23.5 After considering reports from the TAB and the Judicial Commissioner, the Secretary of State may decide to vary, revoke or confirm the effect of the notice. Where the Secretary of State decides to confirm or vary the notice, the IPC must approve the decision. Until the Secretary of State's decision is approved, there is no requirement for the telecommunications operator or postal operator 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 telecommunications operator or postal operator must continue to comply with the notice in relation to the other services covered by the notice.

23.6 Where a technical capability notice is subject to a review the duty to comply in section 66 remains in effect in relation to individual authorisations made under Part 3 of the Act.

23.7 Where a data retention notice applies to more than one telecommunications operator or postal operator then only the operators(s) who referred the notice is exempt from the requirement to comply.

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

24 Keeping of records

Records to be kept by a relevant public authority

24.1 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 IPC.

24.2 These records must be available for inspection by the IPC and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates, particularly where continuing conduct is alleged. 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.

24.3 This code does not affect any other statutory obligations placed on public authorities to keep records under any other enactment - for example the relevant test given in the Criminal Procedure and Investigations Act 1996 and the code of practice under that Act, which 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.

24.4 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 an authorising individual for a decision to obtain communications data (including orally), which were approved after due consideration;

D. the number of applications submitted to an authorising individual 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;

E. the number of authorisations of conduct to acquire communications data granted (not including urgent oral applications);

F. the number of authorisations to give a notice to acquire communications data granted (not including urgent oral applications);

G. the number of notices given pursuant to an authorisation requiring disclosure of communications data (not including urgent oral applications);

H. the number of times an urgent application is approved 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 authorisation for communications data including urgent oral authorisations;

K. whether any part of the authorisation 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 a relevant legislature, or minister of religion) (and if so, which profession)[72];

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)[73].

24.5 These records should distinguish between requests considered by OCDA under section 60A and those considered by designated senior officers under sections 61 and 61A.

24.6 For each **item** of communications data (including consequential 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, authorisation and where relevant the notice;

B. the statutory purpose for which the item of communications data is being sought, as set out at section 60A(7), 61(7) or 61A(7) of the Act;

C. where the item of communications data is being sought for the applicable crime purpose as set out at section 60A(7), 61(7) or 61A(7) of the Act, the crime type being investigated;

D. whether the item of communications data is events or entity, as described at section 261(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[74];

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;

---

[72] See paragraphs 8.8 – 8.45 on communications data involving certain professions for more information.

[73] 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.

[74] The data type is to include whether the data is telephone data, whether fixed line or mobile, or internet data, or postal data. Guidance on specific data types to be collected may be issued by, or sought from the IPC.

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;

H. where an item of data is event data retained by the telecommunications operator or postal operator, an indication of the total number of days of data being sought by means of notice or authorisation[75]; and

I. the telecommunications operator or postal operator from whom the data is being acquired.

24.7 These records must be sent in written or electronic form to the IPC, as requested by them. Guidance on record keeping may be issued by the IPC. Guidance may also be sought by relevant public authorities or persons contracted by them to develop or maintain their information technology systems.

24.8 The IPC 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 telecommunications operator or postal operator (acquisition)

24.9 To assist the IPC to carry out his statutory function in relation to communications data, telecommunications operators and postal operators should maintain a record of the disclosures they have made or been required to make. This record should be available to the IPC and their inspectors to enable comparative scrutiny of the records kept by public authorities. Guidance on the maintenance of records by telecommunications operators and postal operators may be issued by or sought from IPCO.

24.10 The records to be kept by a telecommunications operator or postal operator, in respect of each authorisation should include:

- the identity of the public authority[76];
- the URN of the authorisation;
- the date the relevant details of the authorisation were disclosed to the telecommunications operator or postal operator; and
- the date when the communications data was disclosed to the public authority or, where secure systems are provided by the telecommunications operator or postal operator, the date when the acquisition and disclosure of communications data was undertaken.

24.11 Telecommunications operators and postal operators should also keep sufficient records to be able to provide confirmation of the exact communications data that has been disclosed in the event of later challenge in court. Telecommunications

---

[75] 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.

[76] This can be a code or an abbreviation.

operators and postal operators should retain this data or record 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[77].

24.12 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 telecommunications operator or postal operator (retention)

24.13 To assist the Information Commissioner to carry out their statutory function in relation to the Act, telecommunications operators and postal operators 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 the Commissioner on request.

24.14 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 telecommunications operator or postal operator has fulfilled its responsibilities under chapter 19 regarding security, integrity and destruction of retained data.

24.15 Guidance on the maintenance of records by telecommunications operators and postal operators to assist with the Information Commissioner's statutory functions in relation to the Act may be issued by or sought from him.

Errors

24.16 This section provides information regarding errors, which are not considered to meet the threshold of the offence detailed at paragraph 15.7. Proper application of the Act and thorough procedures for operating its provisions, including for example the careful preparation and checking of applications, notices and authorisations, should reduce the scope for making errors whether by public authorities, telecommunications operators or postal operators

[77] 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.

24.17 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. Wherever possible, technical systems should incorporate functionality to minimise errors.

24.18 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.

24.19 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.

24.20 Where an error results in communications data being acquired or disclosed wrongly, a report must be made to the IPC ('a reportable error') by whoever is responsible for it. For example, the telecommunications operator must report the error if it has resulted from them disclosing data that was not requested, whereas if the error is because the relevant public authority provided incorrect information they must report the 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.

24.21 In cases where an error has occurred but is identified by the public authority or the telecommunications operator or postal operator 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 IPC.

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

24.23 Section 231(9)(a) makes clear that an error can only be a relevant error where it is one that has been made by a public authority in complying with any requirements imposed by the Act (or any other enactment), which are subject to review by the IPC. Section 231(9)(b) sets out that a relevant error must also be one of a description outlined in a Code of Practice under Schedule 7 to the Act. 'A reportable error' made by a public authority as set out in this paragraph 24.24 of this code constitutes a relevant error for the purposes of section 231 of the Act.

24.24 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 telecommunications operator or postal operator when complying with a request under Part 3 of the Act;
- 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 telecommunications operator or postal operator 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[78];
- failure to cancel a requirement to acquire or obtain data as soon as possible once it is known to be no longer valid;
- failure to serve written notice (or where appropriate an authorisation) upon a telecommunications operator or postal operator 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 telecommunications operator or postal operator without data being acquired or disclosed wrongly; and
- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is not acquired or disclosed.

24.25 When a reportable error has occurred, the public authority which made the error, or established that the error had been made, must report the error to the authority's senior responsible officer and then to the IPC within no more than five working days of it being established that an error has occurred. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full.

24.26 Where a public authority reports an error made by a telecommunications operator or postal operator, the public authority should also inform the telecommunications operator or postal operator and IPC of the report in written or electronic form. This will enable the telecommunications operator or postal operator and IPC to investigate the cause or causes of the reported error.

24.27 A full report must be sent to the IPC as soon as reasonably practicable in relation to any reportable error, including details of the error, the public authority's unique reference number of the relevant authorisation, an explanation of how the error occurred, whether any unintended collateral intrusion has taken place and details of

[78] 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.

any remedial action taken including steps taken, or to be taken, to prevent recurrence.

24.28 Where a public authority reports an error made by a telecommunications operator or postal operator, the report must include details of the error and indicate whether the telecommunications operator or postal operator has been informed or not (in which case the public authority must explain why the telecommunications operator or postal operator has not been informed of the report).

24.29 Where a telecommunications operator or postal operator discloses communications data in error, it must report each error to the IPC 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 telecommunications operator or postal operator to do so, identifying the error by reference to the public authority's unique reference number and providing details of any remedial action taken including steps taken, or to be taken, to prevent recurrence. 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.

24.30 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.

24.31 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 telecommunications operator or postal operator, 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 IPC has been made.

24.32 Communications identifiers can be readily transferred, or 'ported', between telecommunications operators. When a correctly completed authorisation or notice results in a telecommunications operator or postal operator indicating to a public authority that, for example, a telephone number has been 'ported' to another telecommunications operator, that authorisation or notice will not constitute an error – unless the fact of the porting was already known to the public authority.

Serious errors

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

24.34 In deciding whether he considers that it is in the public interest for the person concerned to be informed of the serious error, the IPC 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.

24.35 Before making his or her decision, the IPC must require the public authority which has made the error to make submissions on the matters above. Public authorities must take all reasonably practicable steps notified to them by the IPC to identify the subject of a serious error.

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

Excess Data

24.37 Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a telecommunications operator or postal operator in order to comply with the requirement of a notice, the excess data acquired or disclosed should only be retained by the public authority where appropriate to do so – for example in relation to a criminal investigation.

24.38 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.

24.39 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 authorising 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 relevant data protection legislation must also be adhered to in relation to any excess data.

Reporting of errors to the Information Commissioner

24.40 Telecommunications operators and postal operators are only required to report errors made in response to authorisations or notices for communications data under Part 3 to the IPC. The IPC 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.

24.41 The IPC and the Information Commissioner should agree the circumstances under which information on errors should be forwarded.

25 Oversight

The Investigatory Powers Commissioner

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

25.2 The IPC, and those that work under the authority of the IPC, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The IPC may undertake these inspections, as far as they relate to their statutory functions, entirely on his or her own initiative. Section 236 provides for the Intelligence and Security Committee of Parliament to refer a matter to the IPC with a view to carrying out an investigation, inspection or audit.

25.3 The IPC will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the IPC must not act in a way which is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK (see section 229(6)). The IPC must in particular not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, nor unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces (see section 229(7)).

25.4 All relevant persons using investigatory powers must provide all necessary assistance to the IPC and anyone who is acting on behalf of the IPC. Here, a relevant person includes, among others, any person who holds, or has held, an office, rank or position with a public authority (see section 235(7)).

25.5 Anyone including anyone working for a public authority, or a telecommunications operator who has concerns about the way that investigatory powers are being used may report their concerns to the IPC. In particular, any person who exercises the powers described in the Act or this code must, in accordance with the procedure set out in Chapter 24 of this code, report to the IPC any relevant error of which it is aware. This may be in addition to the person raising concerns through the internal mechanisms within the public authority.

25.6 Should the IPC uncover, or be made aware of, what they consider to be a serious error relating to a person who has been subject to an investigatory power then, if it is in the public interest to do so, the IPC is under a duty to inform the person affected. Further information on errors can be found in Chapter 24 of this code. The public authority who has made the error will be able to make representations to the IPC before the IPC decides whether it is in the public interest for the person to be

informed. Section 231(6) states that the IPC must also inform the affected person of any rights that the person may have to apply to the Investigatory Powers Tribunal.

25.7 The IPC must annually report on the findings of their audits, 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 public interest. Only the Prime Minister will be able to make redactions to the IPC's report.

25.8 The IPC may also report, at any time, on any of his or her investigations and findings as they see fit. Public authorities, telecommunications operators and postal operators may seek general advice from the IPC on any issue which falls within the IPC's statutory remit. The IPC may also produce whatever guidance they deem appropriate for public authorities on how to apply and use investigatory powers.

25.9 Further information about the IPC, their office and their work may be found at: www.ipco.org.uk.

The Information Commissioner

25.10 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. Data is retained by virtue of Part 4 where the retention of that data is specifically required by a retention notice. There will be circumstances where the data might be stored in different systems across a CSP's network, for example for business purposes as well as in a dedicated retention store. In such circumstances, the ICO must audit any system that the telecommunications operator or postal operator uses to comply with the retention requirements in a data retention notice.

25.11 Where data is retained as a consequence of a data retention notice but the telecommunications operator or postal operator has a lawful reason to move or copy the data to a separate store, data retained in the separate store, insofar as it is no longer being retained in order to comply with a retention notice, is not subject to audit by the Information Commissioner under the Act. These circumstances may include where a copy of retained data that has been disclosed under Part 3 of the Act is being kept in the event of later challenge in court.[79] Such data must still be kept securely and will be subject to relevant data protection legislation. However, it is not subject to audit by the Information Commissioner under the Act because the lawful basis for retaining the data will no longer be a retention notice.

25.12 Where data retained under a retention notice is moved to another store and kept for a separate lawful purpose, details of the lawful basis for moving the data and keeping it in a separate store, along with details of the process used, must be kept by the telecommunications operator or postal operator and provided to the Information Commissioner on request. This is to ensure that the Information Commissioner can determine that any processes for accessing retained data comply with the security requirements.

25.13 This code does not cover the exercise of the Information Commissioner's functions. It is the duty of any telecommunications operator or postal operator subject to a notice under the Act to comply with any requests made by the Commissioner, in

[79] See paragraph 24.11

order to provide any information required by the Commissioner to discharge their 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.

25.14 Without prejudice to the independence of the Information Commissioner, a telecommunications operator or postal operator may discuss a request from the Commissioner and its potential implications with the Home Office.

25.15 Reports made by the Information Commissioner concerning the inspection of telecommunications operators and postal operators and the security, integrity and destruction of communications data retained under the Act may 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 telecommunications operators and postal operators. The Home Office will work with telecommunications operators and postal operators to address any recommendations made by the Information Commissioner.

25.16 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 telecommunications operators' and postal operators' 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.

25.17 Section 95(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

25.18 The Act imposes a duty on telecommunications operators and postal operators to comply with requirements or restrictions imposed by the Act or a retention notice issued under the Act (see chapter 21). That duty is enforceable by civil proceedings brought by the Secretary of State.

25.19 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 telecommunications operators and postal operators to address any issues identified in the first instance.

25.20 Additionally, should the Information Commissioner establish instances of failure to comply with relevant data protection legislation, he may take enforcement action using powers under that legislation.

25.21 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 telecommunications operator or

postal operator. Chapter 21 of this code sets out the requirements on telecommunications operators and postal operators in relation to any such errors.

26 Contacts / Complaints

General enquiries relating to communications data retention and acquisition

26.1 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

Complaints

Data security, integrity and destruction

26.2 The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with the Act. 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

26.3 The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers, including those covered by this code, as well as conduct by or on behalf of any of the intelligence services and is the only appropriate tribunal for human rights claims against the intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

26.4 The IPT is entirely independent from Her Majesty's Government and the public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint or claim from a person, 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. A 'person' for these purposes includes any organisation and any association or combination of persons (see section 81(1) of RIPA), as well as an individual.

26.5 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

26.6 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 2016 relating to the acquisition of communications data by public authorities and its disclosure by telecommunications operators and postal operators, and to the retention of communications data by such operators.

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
- staff within telecommunications operators and postal operators who are involved in the lawful disclosure of communications data or who currently, or may in the future, retain data under the Act.