DRAFT

Home Office

Acquisition and Disclosure of Communications Data

Draft Code of Practice

Presented to Parliament under section 71 of the Regulation of Investigatory Powers Act 2000

CONTENTS

9. Complaints

INTRODUCTION

1.1 This code of practice relates to the powers and duties conferred or imposed under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 ('the Act'). It provides guidance on the procedures to be followed when acquisition of communications data takes place under those provisions.

1.2 This code applies to relevant public authorities within the meaning of the Act: those listed in section 25 or specified in orders made by the Secretary of State under section 25.[1]

1.3 Relevant public authorities for the purposes of Chapter II of Part I of the Act ('Chapter II') should not:

- use other statutory powers to obtain communications data from a postal or telecommunications operator unless that power provides explicitly for obtaining communications data[2], or is conferred by a warrant or order issued by the Secretary of State or a person holding judicial office, or

- require, or invite, any postal or telecommunications operator to disclose communications data by exercising any exemption to the principle of non-disclosure of communications data under the Data Protection Act 1998 ('the DPA').

1.4 This code should be readily available to members of a relevant public authority involved in the acquisition of communications data and the exercise of powers to do so under the Act, and to communications service operators involved in the disclosure of communications data to public authorities under duties imposed by the Act.[3]

[1] See paragraph 2.10
[2] For example, the power available to Ofcom under section 128 of the Communications Act 2003 to assess whether companies are or have been misusing an electronic communications network or electronic communications service. The purpose for which those assessments are undertaken falls outside the scope of section 22(2) of the Act. See also paragraph 3.23
[3] See section 22(6) of the Act

1.5 Throughout this code an operator who provides a postal or telecommunications service is described as a communications service provider ('CSP'). The meaning of telecommunications service is defined in the Act[4] and extends to CSPs providing such services where the system for doing so is wholly or partly in the United Kingdom or elsewhere. This includes, for example, a CSP providing a telecommunications system to persons in the United Kingdom where communications data relating to that system is either, or both, processed and stored outside the United Kingdom.

1.6 The Act provides that the code is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to a question before any court or tribunal hearing any such proceedings, or to the Tribunal established under the Act[5], or to one of the Commissioners responsible for overseeing the powers conferred by the Act, it must be taken into account.

1.7 The exercise of powers and duties under Chapter II is kept under review by the Interception of Communications Commissioner ('the Commissioner') appointed under section 57 of the Act and by his inspectors who work from the Interception of Communications Commissioner's Office (IOCCO).

1.8 This code *does not* relate to the interception of communications nor to the acquisition or disclosure of the contents of communications. The Code of Practice on Interception of Communications issued pursuant to Section 71 of the Act provides guidance on procedures to be followed in relation to the interception of communications.[6]

1.9 Communications data that is obtained directly as a consequence of the execution of an interception warrant ('related communications data'[7]) is intercept product.

---

[4] Sections 2(1) and 81(1) of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service); and defines 'telecommunications system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.

[5] See paragraphs 9.1 and 9.2

[6] ISBN 0-11-341281-9

[7] Section 20 of the Act defines 'related communications data' in relation to a communication intercepted in the course of its transmission, by means of a postal service or telecommunications system, to mean so much of any communications data (within the meaning of Chapter II of Part I of the Act) as–

(a) is obtained by, or in connection with, the interception; and
(b) relates to the communication or to the sender or recipient, or intended recipient, of the communication.

1.10 Any related communications data, and any other specific communications data ('other related data') derived directly from it, must be treated in accordance with the restrictions on the use of intercepted material and related communications data.[8]

1.11 Related communications data may be used as a basis for the acquisition of other related data for intelligence purposes[9] only, if there is sufficient intercept product or non-intercept material available to a designated person to allow that person to consider the necessity and proportionality of acquiring the other related data. The application to the designated person[10] and the resultant data acquired should be treated as product of the interception.

1.12 Related communications data may be used as a basis for the acquisition of other related data for use in legal proceedings provided that the related communications data does not identify itself as intercept product and there is sufficient non-intercept material available to the designated person to allow that person to consider the necessity and proportionality of acquiring the other related data. In practice it will be rare to achieve this. Consequently, it is best practice when undertaking the acquisition of other related data for use in legal proceedings that the provenance of such data is from a source other than conduct authorised by an interception warrant.

1.13 This code extends to the United Kingdom.[11]

[8] See sections 15, 17, 18 and 19 of the Act

[9] Section 81(5) of the Act qualifies the reference to preventing or detecting serious crime in section 5(3) – grounds for the issue of an interception warrant – to exclude gathering of evidence for use in any legal proceedings.

[10] See paragraph 3.7

[11] This code and the provisions of Chapter II of Part I of the Act do not extend to the Crown Dependencies and British Overseas Territories.

GENERAL EXTENT OF POWERS

Scope of Powers, Necessity and Proportionality

2.1 The acquisition of communications data under the Act will be a justifiable interference with an individual's human rights under Article 8 of the European Convention on Human Rights only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.

2.2 The Act stipulates that conduct to be authorised or required must be necessary for one or more of the purposes set out in section 22(2) of the Act:[12]

- in the interests of national security;[13]
- for the purpose of preventing or detecting crime[14] or of preventing disorder;
- in the interests of the economic well-being of the United Kingdom;[15]
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

[12] The Act permits the Secretary of State to add further purposes by means of an Order subject to the affirmative resolution procedure in Parliament.

[13] One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. These functions extend throughout the United Kingdom. A designated person in another public authority should not grant an authorisation or give a notice under the Act where the operation or investigation falls within the responsibilities of the Security Service, as set out above, except where the conduct is to be undertaken by a Special Branch, by the Metropolitan Police Counter Terrorism Command, or where the Security Service has agreed that another public authority can acquire communications data in relation to an operation or investigation which would fall within the responsibilities of the Security Service.

[14] Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed. See section 81(5) of the Act. 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 Chapter II to obtain communications data for the purpose of preventing and detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain communications data under the Act.

[15] See paragraph 2.11

- for the purpose, in an emergency, 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;[16]

- for the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime (such as a natural disaster or an accident),[17] and

- in relation a person who has died or is unable to identify himself, for the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for his death or condition.[18]

2.3 The purposes for which some public authorities may seek to acquire communications data are restricted by order.[19] The designated person may only consider necessity on grounds open to his or her public authority and only in relation to matters that are the statutory or administrative function of their respective public authority.

2.4 There is a further restriction upon the acquisition of communications data:

- in the interests of public safety;

- for the purpose of protecting public health;

- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

Only communications data within the meaning of section 21(4)(c) of the Act may be acquired for these purposes and only by those public authorities permitted by order to acquire communications data for one or more of those purposes.[20]

[16] See article 2 (a), SI 2006/1878
[17] See article 2 (b) (i), SI 2006/1878
[18] See article 2 (b) (ii) SI 2006/1878
[19] See article 6, SI 2003/3172
[20] See article 7, SI 2003/3172

2.5 The designated person must believe that the conduct required by any authorisation or notice is necessary. He or she must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communication data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the intrusiveness of the interference with an individual's right of respect for their private life against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

2.6 Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation. An application for the acquisition of communications data should draw attention to any circumstances which give rise to a meaningful degree of collateral intrusion.

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

2.8 Any conduct that is excessive in the circumstances of both the interference and the aim of the investigation or operation, or is in any way arbitrary will not be proportionate.

2.9 Exercise of the powers in the Act to acquire communications data is restricted to designated persons in relevant public authorities. A designated person is someone holding a prescribed office, rank or position within a relevant public authority that has been designated for the purpose of acquiring communications data by order.[21]

2.10 The relevant public authorities for Chapter II are set out in section 25(1). They are:

- a police force (as defined in section 81(1) of the Act);[22]
- the Serious Organised Crime Agency;[23]
- HM Revenue and Customs;[24]
- the Security Service;

[21] See articles 2 and 4, SI 2003/3172. By virtue of article 5 of the order all more senior personnel to the designated office, rank or position are also allowed to grant authorisations or give notices.
[22] Each police force is a separate relevant public authority which has implications for the separation of roles in the acquisition of data under the Act.
[23] References in the Act to the National Criminal Intelligence Service and the National Crime Squad have been amended by the Serious Organised Crime and Police Act 2005.
[24] References in the Act to HM Customs and Excise and Inland Revenue have been amended by the Commissioners for Revenue and Customs Act 2005.

- the Secret Intelligence Service;

- the Government Communications Headquarters.

These and additional relevant public authorities are listed in schedules to the Regulation of Investigatory Powers (Communications Data) Order 2003[25] and the Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2005[26], the Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006[27]and any similar future orders made under section 25 of the Act.

2.11 Where acquisition of communications data is necessary in the interests of the economic well-being of the United Kingdom, a designated person must take into account whether the economic well-being of the United Kingdom is, on the facts of the specific case, directly related to State security. The term "State security", which is used in Directive 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector), should be interpreted in the same way as the term "national security" which is used elsewhere in the Act and this code.

Communications Data

2.12 The code covers any conduct relating to the exercise of powers and duties under Chapter II of Part I of the Act to acquire or disclose communications data. Communications data is defined in section 21(4) of the Act.

2.13 The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content, not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video (with the exception of traffic data to establish another communication such as that created from the use of calling cards, redirection services, or in the commission of 'dial through' fraud and other crimes where data is passed on to activate communications equipment in order to obtain communications services fraudulently).

[25] SI 2003/3172 *www.opsi.gov.uk/si/si2003/20033172.htm*
[26] SI 2005/1083 *www.opsi.gov.uk/si/si2005/20051083.htm*
[27] SI 2006/1878 *www.opsi.gov.uk/si/si2006/20061878.htm*

2.14 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services, those being postal services[28] or telecommunications services.[29]

2.15 Communications service providers may therefore 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 hotels, restaurants, libraries and airport lounges.

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

2.17 Consultation with the public authority's Single Point of Contact (SPoC)[30] will determine the most appropriate plan for acquiring data where the provision of a communication service engages a number of providers.

2.18 Any conduct to determine the communications service provider that holds, or may hold, specific communications data is not conduct to which the provisions of Chapter II 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 internet protocol address.

[28] Sections 2(1) and 81(1) of the Act define 'postal service' to mean any service which consists in the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items and 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.
[29] See footnote 4
[30] See paragraph 3.15

Traffic Data

2.19 The Act defines certain communications data as 'traffic data' in sections 21(4)(a) and 21(6) of the Act. This is data that is or has been comprised in or attached to a communication for the purpose of transmitting the communication and which 'in relation to any communication':

- identifies, or appears to identify, any person, equipment[31] or location to or from which a communication is or may be transmitted;
- identifies or selects, or appears to identify or select, transmission equipment;
- comprises signals that activate equipment used, wholly or partially, for the transmission of any communication (such as data generated in the use of carrier pre-select or redirect communication services or data generated in the commission of, what is known as, 'dial through' fraud);
- identifies data as data comprised in or attached to a communication. This includes data which is found at the beginning of each packet in a packet switched network that indicates which communications data attaches to which communication.

2.20 Traffic data includes data identifying a computer file or a computer program to which access has been obtained, or which has been run, by means of the communication – but only to the extent that the file or program is identified by reference to the apparatus in which the file or program is stored. In relation to internet communications, this means traffic data stops at the apparatus within which files or programs are stored, so that traffic data may identify a server or domain name (web site) but not a web page.

[31] In this code equipment has the same meaning as 'apparatus', which is defined in section 81(1) of the Act to mean 'any equipment, machinery, device, wire or cable'.

2.21 Examples of traffic data, within the definition in section 21(6), include:

- 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 equipment when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed;
- 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;
- record of correspondence checks comprising details of traffic data from postal items in transmission to a specific address, and
- online tracking of communications (including postal items and parcels).

2.22 Any message written on the outside of a postal item, which is in transmission, may be content (depending on the author of the message) and fall within the scope of the provisions for interception of communications. For example, a message written by the sender 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 traffic data within section 21(4)(a) of the Act.

Service Use Information

2.23 Data relating to the use made by any person of a postal or telecommunications service, or any part of it, is widely known as 'service use information' and falls within section 21(4)(b) of the Act.

2.24 Service use information is, or can be, routinely made available by a CSP to the person who uses or subscribes to the service to show the use of a service or services and to account for service charges over a given period of time. Examples of data within the definition at section 21(4)(b) include:

- itemised telephone call records (numbers called[32]);
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about the use of forwarding/redirection services;
- information about selection of preferential numbers or discount calls;
- records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

[32] 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.

Subscriber Information

2.25 The third type of communication data, widely known as 'subscriber information', is set out in section 21(4)(c) of the Act. This relates to information held or obtained by a CSP about persons[33] to whom the CSP provides or has provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it.

2.26 Examples of data within the definition at section 21(4) (c) include:

- 'subscriber checks' (also known as 'reverse look ups') such as "who is the subscriber of phone number 012 345 6789?", "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*?";
- 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;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes;[34]

[33] Section 81(1) of the Act defines 'person' to include any organisation and any association or combination of persons.

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

- information provided by a subscriber or account holder to a CSP, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is *not* disclosed save where the requirement for such information is necessary in the interests of national security[35]).

2.27 It can be appropriate to undertake the acquisition of subscriber information before obtaining related traffic data or service use information to confirm information within the investigation or operation.

2.28 Where there is sufficient provenance of information within the investigation or operation to justify an application to obtain traffic data or service use information in the first instance this may be undertaken. For example, in circumstances where:

- a victim reports receiving nuisance or threatening telephone calls or messages;
- a person who is subject of an investigation or operation is identified from high-grade intelligence to be using a specific communication service;
- a victim, a witness or a person who is subject of an investigation or operation has used a public payphone;[36]
- a person who is subject of an investigation or operation is identified during a time critical investigation (such as a kidnap) or from detailed analysis of data available to the investigator to be using a specific communication service;
- a mobile telephone is lawfully seized and communications data is requested relating to either or both the device or its SIM card(s);
- a witness presents certain facts and there is a need to corroborate or research the veracity of those, such as to confirm the time of an incident they have witnessed, or
- an investigation of the allocation of IP addresses is needed to determine relevant subscriber information.

[35] Information which provides access to the content of any stored communications may only be used for that purpose with necessary lawful authority.
[36] 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.

2.29 Where the acquisition of the subscriber information is required to assist an investigation or operation or for evidential purposes, that requirement can be included on an application for traffic data or service use information.

GENERAL RULES ON THE GRANTING OF AUTHORISATIONS AND GIVING OF NOTICES

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

- the applicant
- the designated person
- the single point of contact
- the senior responsible officer

3.2 The Act provides two alternative means for acquiring communications data, by way of:

- an authorisation under section 22(3), or
- a notice under section 22(4).

The applicant

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

3.4 Applications may be made orally in exceptional circumstances[37], but a record of that application must be made in writing or electronically as soon as possible.

3.5 Applications[38] – the original or a copy of which must be retained by the SPoC within the public authority – must:

- include the name (or designation[39]) and the office, rank or position held by the person making the application;

- include a unique reference number;

[37] See paragraph 3.56

[38] Public authorities should ensure their application processes are efficient and do not impose unnecessary bureaucracy on their operational staff which goes beyond the requirements of the Act and this code. To assist public authorities the Home Office publishes specimen forms.

[39] The use of a designation rather than a name will be appropriate only for applicants in one of the security and intelligence agencies.

- include the operation name (if applicable) to which the application relates;

- specify the purpose for which the data is required, by reference to a statutory purpose under 22(2) of the Act;

- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);

- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;

- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances, and

- identify and explain the time scale within which the data is required.[40]

3.6 The application should record subsequently whether it was approved or not by a designated person, and by whom and when that decision was made. If approved, the application form should, to the extent necessary, be cross-referenced to any authorisation granted[41] or notice given.

[40] The Data Communications Group (DCG) which comprises representatives of CSPs, UK law enforcement and other public authorities to manage the strategic relationship between public authorities and the communications industry has adopted a grading scheme to indicate the appropriate timeliness of the response to requirements for disclosure of communications data. There are three grades:

- Grade 1 – an immediate threat to life;
- Grade 2 – an exceptionally urgent operational requirement for the prevention or detection of serious crime or a credible and immediate threat to national security;
- Grade 3 – matters that are routine but, where appropriate, will include specific or time critical issues such as bail dates, court dates, or where persons are in custody or where a specific line of investigation into a serious crime and early disclosure by the CSP will directly assist in the prevention or detection of that crime

The emphasis within Grade 1 and 2 is the urgent provision of the communications data will have an immediate and positive impact on the investigation or operation.

[41] Cross-referencing will be unnecessary in circumstances where the grant of an authorisation is recorded in the same document as the relevant application.

The designated person

3.7 The designated person is a person holding a prescribed office in a relevant public authority who considers the application and records his considerations at the time (or as soon as is reasonably practicable) in writing or electronically. If the designated person believes it is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given.

3.8 Individuals who undertake the role of a designated person must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data under Chapter II and this code.

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

3.10 The designated person shall assess the necessity for any conduct to acquire or obtain communications data taking account of any advice provided by the single point of contact (SPoC).

3.11 Designated persons should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons. Where a designated person is directly involved in the investigation or operation their involvement and their justification for undertaking the role of the designated person must be explicit in their recorded considerations.

3.12 Particular care must be taken by designated persons when considering any application to obtain communications data to identify equipment (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 equipment is unknown.[42] Unless the application is based on information that the equipment 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.

[42] DCG is able to offer additional advice to SPoCs where investigations or operations in their public authority are considering the acquisition of such data.

3.13 In situations where there is an immediate threat to life (for example a person threatening to take their own or someone else's life or where threats are made to a victim in a kidnap) some CSPs will undertake to bespoke their systems beyond the requirements of their normal business practice to be able to assist the police 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.

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

The single point of contact

3.15 The single point of contact (SPoC) is either an accredited individual or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued a SPoC Personal Identification Number (PIN). Details of all accredited individuals are available to CSPs for authentication purposes.

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

3.17 The SPoC[43] should be in a position to:

- engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations;

- assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;[44]

[43] 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.

- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;

- advise applicants and designated persons on the interpretation of the Act, particularly whether an authorisation or notice is appropriate;

- provide assurance to designated persons that authorisations and notices are lawful under the Act and free from errors;

- provide assurance to CSPs that authorisations and notices are authentic and lawful;

- assess whether communications data disclosed by a CSP in response to a notice fulfils the requirement of the notice;

- assess whether communications data obtained by means of an authorisation fulfils the requirement of the authorisation;

- assess any cost and resource implications to both the public authority and the CSP of data requirements.

3.18 Public authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of communications data. In circumstances where a CSP is approached by a person who cannot be authenticated as an accredited individual and who seeks to obtain data under the provisions of the Act, the CSP may refuse to comply with any apparent requirement for disclosure of data until confirmation of the person's accreditation and PIN is obtained from the Home Office.

3.19 The SPoC may be an individual who is also a designated person. The SPoC may be an individual who is also an applicant. The same person should never be an applicant, a designated person and a SPoC. Equally the same person should never be both the applicant and the designated person.

3.20 Where a public authority seeks to obtain communications data using provisions providing explicitly for the obtaining of communications data (other than Chapter II of Part I of the Act) or using statutory powers conferred by a warrant or order issued by the Secretary of State or a person holding judicial office, the SPoC should be engaged in the process of obtaining the data to ensure effective co-operation between the public authority and the CSP.

---

[44] In the event that the required data is inextricably linked to, or inseparable from, other traffic data or service use data the designated person must take that into account in their consideration of necessity, proportionality and collateral intrusion.

3.21 Similarly, where a public authority seeks lawful access to the content of a stored communication held by a CSP or to data held by a CSP that is neither communications data or the content of a communication, the SPoC should be engaged to liaise with the CSP[45] (for example to obtain access to a deceased's voicemail).

The senior responsible officer

3.22 Within every relevant public authority a senior responsible officer[46] must be responsible for:

- the integrity of the process in place within the public authority to acquire communications data;
- compliance with Chapter II of Part I of the Act and with this code;
- oversight of the reporting of errors to IOCCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the IOCCO inspectors when they conduct their inspections, and
- where necessary, oversee the implementation of post-inspection action plans approved by the Commissioner.

[45] Sections 1(5)(c), 2(7), 2(8), 3(1) and 3(2) of the Act explain how stored communications may be in the course of their transmission and may be lawfully intercepted without a warrant.

[46] The senior responsible officer should be a person holding the office, rank or position of a designated person within the public authority who may authorise communications falling within section 21(4)(a) and or 21(4)(b).

Authorisations

3.23 An authorisation provides for persons within a public authority to engage in specific conduct, relating to a postal service or telecommunications system, to obtain communications data.

3.24 Any designated person in a public authority may only authorise persons working in the same public authority to engage in specific conduct. This will normally be the public authority's SPoC.

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

3.26 An authorisation may be appropriate where:

- a CSP is not capable of obtaining or disclosing the communications data;[47]
- there is an agreement in place between a public authority and a CSP relating to appropriate mechanisms for disclosure of communications data, or
- a designated person considers there is a requirement to identify a person to whom a service is provided but a CSP has yet to be conclusively determined as the holder of the communications data.

3.27 An authorisation is not served upon a CSP, although there may be circumstances where a CSP may require or may be given an assurance that conduct being, or to be, undertaken is lawful. That assurance may be given by disclosing details of the authorisation or the authorisation itself.

3.28 An authorisation[48] – the original or a copy of which must be retained by the SPoC within the public authority – must:

- be granted in writing or, if not, in a manner that produces a record of it having been granted;
- 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);

[47] Where possible, this assessment will be based upon information provided by the CSP.
[48] Where the grant of an authorisation is recorded separately from the relevant application they should be cross-referenced to each other.

- specify the purpose for which the conduct is authorised, by reference to a statutory purpose under section 22(2) of the Act;

- specify the office, rank or position held by the designated person granting the authorisation. The designated person should also record their name (or designation) on any authorisation they grant, and

- record the date and, when appropriate to do so, the time[49] when the authorisation was granted by the designated person.

3.29 SPoCs should be mindful when drafting authorisations within the meaning of section 23(1) of the Act to ensure the description of the required data corresponds with the way in which the CSP processes, retains and retrieves its data for lawful disclosure. CSPs cannot necessarily or reasonably edit or bespoke their systems to take account of every possible variation of what may be specified in authorisations.

3.30 Requirements to identify a person to whom a service is, or has been, provided – for example telephone number subscriber checks – account for the vast majority of disclosures under the Act. As a consequence of these requirements, some CSPs permit the lawful acquisition of this data by SPoCs, subject to security and audit controls. Where a SPoC has been authorised to engage in conduct to obtain details of a person to whom a service has been provided and concludes that data is held by a CSP from which it cannot be acquired directly, the SPoC may provide the CSP with details of the authorisation granted by the designated person in order to seek disclosure of the required data.[50]

3.31 At the time of giving a notice or granting an authorisation to obtain specific traffic data or service use data, a designated person may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of specific subscriber information relating to the traffic data or service use 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 to whom the target of an investigation or operation was observed to make several calls from a public pay phone;

[49] Recording of the time an authorisation is granted (or a notice is given) will be appropriate in urgent and time critical circumstances.

[50] Where details of an authorisation are provided to a CSP in writing, electronically or orally those details must additionally specify the manner in which the data should be disclosed and, where appropriate, provide an indication of any urgency or time within which the data need to be obtained.

- to identify a person making unlawful and unwarranted demands (as in the case of kidnap, extortion and blackmail demands and threats of violence), and

- 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.

3.32 It is the duty of the senior responsible officer to ensure that the designated person, applicant or other person makes available to the SPoC such information as the senior responsible officer thinks necessary to ensure the integrity of any requirements for the acquisition of subscriber information to be obtained directly upon the acquisition or disclosure of any traffic data or service use data, and their compliance with Chapter II and with this code.[51]

Notices

3.33 Giving of a notice is appropriate where a CSP is able to retrieve or obtain specific data, and to disclose that data, unless the grant of an authorisation is more appropriate. A notice may require a CSP to obtain any communications data, if that data is not already in its possession.

3.34 The decision of a designated person whether to give a notice shall be based upon information presented to them in an application.

3.35 The 'giving of a notice' means the point at which a designated person determines that a notice should be given to a CSP. In practice, subsequent to the designated person giving that notice it is served upon a CSP whether in writing or, in an urgency, orally.

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

3.37 A notice – the original or a copy of which must be retained by the SPoC within the public authority – must:

- be given in writing[52] or, if not, in a manner that produces a record, within the public authority, of its having been given;

[51] 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 traffic data or service use information from which the data are derived.

[52] The preparation and format of a notice must take into account that when served on a CSP by the use of a facsimile machine or other means the notice remains legible.

- include a unique reference number and also identify the public authority;[53]

- specify the purpose for which the notice has been given, by reference to a statutory purpose under 22(2) of the Act;

- 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);

- include an explanation that compliance with the notice is a requirement of the Act;

- specify the office, rank or position held by the designated person giving the notice. The name (or designation) of the designated person giving the notice should also be recorded;

- specify the manner in which the data should be disclosed. The notice should contain sufficient information including the contact details of the SPoC to enable a CSP to confirm the notice is authentic and lawful;

- record the date and, when appropriate to do so, the time when the notice was given by the designated person, and

- where appropriate, the notice should provide an indication of any urgency or time within which the CSP is requested to comply with the requirements of the notice.[54]

3.38 A notice must not place a CSP under a duty to do anything which is not reasonably practicable for the CSP to do.[55] SPoCs should be mindful when drafting notices to ensure the description of the required data corresponds with the ways in which the CSP processes, retains and retrieves its data for lawful disclosure. CSPs cannot necessarily or reasonably edit or bespoke their systems to take account of every possible variation of what may be specified in notices.

3.39 In giving notice a designated person may only require a CSP to disclose the communications data to the designated person or to a specified person working within the same public authority. This will normally be the public authority's SPoC.

[53] 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.
[54] See footnote 40
[55] See Section 22(7) of the Act

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

3.41 Where the designated person determines, if necessary upon the advice of the SPoC, that there are specific circumstances which mean that if a notice were given the CSP could not comply within ten working days the designated person shall indicate such longer period as the notice may specify up to a period of one month from the date notice is given.[56]

Duration of authorisations and notices

3.42 Relevant to all authorisations and notices is the date upon which authorisation is granted or notice given. From that date, when the authorisation or notice becomes valid, it has a validity of a maximum of one month.[57] This means the conduct authorised should have been commenced or the notice served within that month.

3.43 All authorisations and notices should refer to the acquisition or disclosure of data relating to a specific date or period.[58] Any period should be clearly indicated in the authorisation or notice. The start date and end date should be given, and where a precise start and end time are relevant these must be specified.[59] 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 or the notice given by the designated person. 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'.

3.44 Where an authorisation or a notice 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 or the notice given.

---

[56] Where a CSP required to disclose communications data is unable ordinarily to comply within 10 working days, a senior officer of the CSP should seek an interim service level agreement with the Home Office.

[57] 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.

[58] For example, details of traffic data or service use on a specific date or for a specific period or the details of a subscriber on a specific date or for a specific period.

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

3.45 Designated persons should give particular consideration to any periods of days or shorter periods of time for which they may approve for the acquisition or disclosure of historic or future data. They should specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise will impact on the proportionality of the authorisation or notice and impose unnecessary burden upon a CSP given such notice.

Renewal of authorisations and notices

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

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

3.48 Where a designated person is granting a further authorisation or giving a further notice to renew an earlier authorisation or notice[60], the designated person should:

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

Cancellation of notices and withdrawal of authorisations

3.49 A designated person who has given notice to a CSP under section 22(4) of the Act shall cancel the notice if, at any time after giving the notice[61], it is no longer necessary for the CSP to comply with the notice or the conduct required by the notice is no longer proportionate to what was sought to be achieved.

[60] This can include an authorisation or notice that has been renewed previously.
[61] This can include a renewed notice.

3.50 Reporting the cancellation of a notice to a CSP shall be undertaken by the designated person directly or, on that person's behalf, by the public authority's SPoC. Where human rights considerations are such that a notice should be cancelled with immediate effect the designated person or the SPoC will notify the CSP.[62]

3.51 Cancellation of a notice reported to a CSP must:

- be undertaken in writing or, if not, in a manner that produces a record of the notice having been cancelled;
- identify, by reference to its unique reference number, the notice being cancelled; and
- record the date and, when appropriate to do so, the time when the notice was cancelled.

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

3.53 Similarly where a designated person considers an authorisation[63] should cease to have effect, because the conduct authorised becomes unnecessary or no longer proportionate to what was sought to be achieved, the authorisation must be withdrawn. It may be the case that it is the SPoC who is first aware that the authorisation is no longer necessary or proportionate and may cease the authorised conduct, and then inform the designated person who granted the authorisation.

3.54 Withdrawal of an authorisation should:

- be undertaken in writing or, if not, in a manner that produces a record of it having been withdrawn;
- 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

[62] If the notice being cancelled relates to an urgent operational situation that has been resolved, or has changed, it may be appropriate for the senior officer dealing with the situation, on the ground or in a control room, to notify the CSP that the notice is cancelled where that person has the earliest opportunity to do so.
[63] This can include a renewed authorisation.

- record the name and the office, rank or position held by the designated person informed of the withdrawal of the authorisation.

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

Urgent oral giving of notice or grant of authorisation

3.56 In exceptionally urgent circumstances[64], application for the giving of a notice or the grant of an authorisation may be made by an applicant, approved by a designated person and either notice given to a CSP or an authorisation granted orally. Circumstances in which an oral notice or authorisation may be appropriate are:

- an immediate threat to life such that a person's life might be endangered if the application procedure were undertaken in writing from the outset,

- an exceptionally urgent operational requirement where, within no more than 48 hours of the notice being given or the authorisation being granted orally, the acquisition of communications data will directly assist the prevention or detection of the commission of a serious crime[65] and the making of arrests or the seizure of illicit material, and where that operational opportunity will be lost if the application procedure is undertaken in writing from the outset, or

- a credible and immediate threat to national security or a time-critical and unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost, if the application procedure were undertaken in writing from the outset.

3.57 The use of urgent oral process must be justified for each application within an investigation or operation. The fact that any part of an investigation or operation is undertaken urgently must not be taken to mean that all requirements to obtain communications data in connection with that investigation or operation be undertaken using the urgent oral process.

---

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

[65] See section 81(2) of the Act.

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

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

3.60 Written notice[66] must be given to the CSP retrospectively within one working day[67] of the oral notice being given. Failure to do so will constitute an error which may be reported to the Commissioner by the CSP and must be recorded by the public authority.

3.61 After the period of urgency[68], a written process must be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the SPoC shall collate details or copies of control room or other operational logs which provide contemporaneous records of the consideration given to the acquisition of data, decision(s) made by the designated person and the actions taken in respect of the decision(s).

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

[66] Likewise where details of an authorisation are provided to a CSP orally in a matter of urgency, they should be confirmed in writing within one working day.

[67] Working day means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in that part of the United Kingdom where the relevant public authority is located.

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

MAKING OF CONTRIBUTIONS TOWARDS THE COSTS INCURRED BY COMMUNICATIONS SERVICE PROVIDERS

4.1 The Act[69] recognises that CSPs incur costs in complying with notices to disclose communications data, and allows for arrangements for making appropriate payments to them to facilitate the timely disclosure of communications data. In this code 'timely disclosure' means that ordinarily a CSP should disclose data within ten working days of being required to do so. Similar arrangements are appropriate where a CSP incurs costs in making provision for the acquisition of communications data upon the grant of an authorisation under the Act.

4.2 Significant public funding is made available to CSPs to ensure that they can provide, outside of their normal business practices, an effective and efficient response to 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.

4.3 It is legitimate for a CSP to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to comply with notices or to provide for the acquisition and timely disclosure of communications data. This is especially relevant for CSPs which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems. Contributions can also be appropriate towards costs incurred by a CSP which needs to update its systems to maintain, or make more efficient, its disclosure process or 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 made of such services.

4.4 Any CSPs seeking to recover appropriate contributions towards its costs should make available to the Home Office such information or assurance as the Home Office requires to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the CSP.

[69] Section 24 of the Act

SPECIAL RULES ON THE GRANTING OF AUTHORISATIONS AND GIVING OF NOTICES IN SPECIFIC MATTERS OF PUBLIC INTEREST

Sudden deaths, serious injuries and vulnerable persons

5.1 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. Article 2(b) of the Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006 specified additional 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 resulting from crime (such as 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;
- 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.

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

5.3 Equally communications data can help establish the facts relevant to a person's death or serious injury, where no crime has occurred. For example, where the police undertake an investigation to assist Her Majesty's Coroner, communications data can indicate the activity of a deceased person prior to their death, such as in a fatal accident, or identify a person who may assist the Coroner to establish the facts of a person's death.

5.4 Under the Act communications data may also be obtained and disclosed in serious and urgent welfare cases where it is necessary within the meaning of section 22(2)(g) and the conduct authorised or required is proportionate to what is sought to be achieved by obtaining the data.

Public Emergency Call Service (999/112 Calls)

5.5 Certain CSPs have obligations under the Communications Act 2003[70] in respect of emergency calls made to 999 and 112 emergency numbers. They 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.

5.6 Caller location information, which provides the geographic position of the equipment being used by the person making the emergency call, facilitates a fast response in emergency situations where the caller is unable to give their position (for example because the caller does not know, is panicking or is incapacitated).

5.7 Handling of an emergency call involves four phases:

- connection of the caller to the Emergency Operator using the 999/112 number;
- selection by the Emergency Operator of the required Emergency Authority Control Room (Police, Fire, Ambulance or Coastguard)('the emergency service');
- connection of the caller to the Emergency Authority Control Room;
- listening by the Emergency Operator to ensure the caller is connected to the correct emergency service and to provide further assistance to the caller or the emergency service when required.[71]

5.8 Best practice dictates that the emergency operator will disclose location information to the emergency service during the initial call hand-over. In many cases this will be done automatically by the call handling system.

[70] General Conditions of Entitlement set by Ofcom under section 45 of the 2003 Act.
[71] This can also include silent emergency calls where the call is connected but the caller, for whatever reason, is unable to speak to the emergency operator or the emergency service.

5.9 In automated cases, data relating to the emergency call is automatically displayed at the relevant emergency service, the instant a call is routed from the Emergency Operator. This data is available to the emergency service throughout the duration of the emergency call, but disappears once the call has ended unless retained by the emergency service.

5.10 The Privacy and Electronic Communications (EC Directive) Regulations 2003 ('the Privacy Regulations')[72] allows telephone users the choice whether or not their telephone number is displayed or can be accessed by the recipient of a call they make. However when an emergency call using 999 or 112 is made, the option to withhold the number making the call is not available. Instead the calling line identity and location data (fixed or mobile) are automatically disclosed to the emergency services in order to facilitate a rapid response to the emergency call.

Dropped 999/112 calls (and circumstances where data may be acquired or disclosed outside the provisions of the Act)

5.11 To enable the provision of emergency assistance in response to emergency calls which are 'dropped' or incomplete, the emergency service can call upon an Emergency Operator or relevant service provider to disclose data about the maker[73] of an emergency call within the emergency period (within one hour of the termination of the emergency call) outside the provisions of the Act.

5.12 This is necessary in situations where the Emergency Operator may become aware of the premature termination of an emergency call. There are a number of reasons for these 'dropped' or incomplete emergency calls, which cannot be reconnected. For example:

- there is a fault on the line;
- the emergency service requests to be reconnected where the caller was incapacitated or unable to maintain the call and reconnection is tried and fails;
- the emergency service considers that safety of the person making the call may be put at risk if the Emergency Operator seeks to reconnect the call, particularly in cases where a crime is in progress, for example domestic violence or a robbery;

[72] SI 2003/2426 *www.legislation.hmso.gov.uk/si/si2003/20032426.htm* Regulation 10 concerns prevention of calling line identification in relation to outgoing calls.

[73] In practice this means sufficient detail disclosed to identify the origin of the call and, if appropriate, to enable the deployment of an emergency service to the scene of an emergency.

- the Emergency Operator diagnoses a problem with the call or the strength of a mobile phone signal.

5.13 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.

5.14 The Emergency Operator can anticipate the needs of the emergency service and represent the information disclosed automatically to the emergency service without prompting.

5.15 The Emergency Operator can choose to represent the data, whether prompted or unprompted, only for the period of time that the data is held specifically as emergency call data. This period is not normally longer than one hour from the termination of the emergency call.

5.16 There are circumstances where the Emergency Operator cannot automatically present the emergency service with communications data about the maker of an emergency call. For example, because the emergency service does not have equipment to receive the data automatically or the data is held by a third party service provider and not readily available to the Emergency Operator. In those circumstances, and in order to provide an effective emergency service, the Emergency Operator may disclose the data it has orally.

5.17 When disclosure of data about the maker of an emergency call is required during the emergency period, the emergency service controller must provide a unique reference number for the emergency call and provide the name of the authorising officer and sufficient detail to link the disclosure to the originator of the request. Where telephone numbers (or other identifiers) are being relayed, the relevant number must be read twice and repeated back by the CSP to confirm the correct details have been taken.

5.18 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.

5.19 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.

5.20 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.

Malicious and nuisance communications

5.21 Many CSPs offer services to their customers to deal with complaints concerning malicious and nuisance communications.[74] Although these services vary all CSPs believe that such calls can be very distressing for their customers and that every effort should be made to resolve such situations as efficiently and effectively as possible.

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

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

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

5.25 Upon receipt of a complaint a CSP may retrieve and retain relevant specific data that, if appropriate, can be disclosed to the police later. If the complainant wishes the matter to be investigated, it is essential for the CSP and the police[75] to liaise with one another to ensure the lawful disclosure of data to enable any offence to be effectively investigated.

5.26 Where the complainant reports a matter to the police that has been previously raised with the CSP, any data already collated by the CSP may be disclosed to the police SPoC under the provisions of the DPA or the Privacy Regulations.[76] Subsequent police investigation may require the acquisition or disclosure of additional communications data from the complainant's CSP or other CSPs under the provisions of the Act.

---

[74] The Association of Chief Police Officers has produced guidelines on 'Dealing with Malicious and Nuisance Communications'. See *www.acpo.police.uk/policies.asp*

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

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

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

KEEPING OF RECORDS

Records to be kept by a relevant public authority

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

6.2 These records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of the Act, to carry out its functions.[77]

6.3 Where the records contain, or relate to, material obtained directly as a consequence of the execution of an interception warrant those records must be treated in accordance with the safeguards which the Secretary of State has approved in conformity with the duty imposed upon him by the Act.[78]

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

6.5 Each relevant public authority must also keep a record of the following items:

- number of applications submitted to a designated person for a decision to obtain communications data which were rejected after due consideration;

[77] The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is satisfied it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates. See section 67(5) of the Act.
[78] Under section 15 of the Act and the statutory code of practice on Interception of Communications.

- number of notices requiring disclosure of communications data within the meaning of each subsection of section 21(4) of the Act or any combinations of data;

- number of authorisations for conduct to acquire communications data within the meaning of each subsection of section 21(4) of the Act or any combinations of data;

- number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data within the meaning of each subsection of section 21(4) of the Act or any combinations of data.

6.6 This record must be sent in written or electronic form to the Commissioner as determined by him. Where appropriate, guidance on format or timing may be issued by or sought from IOCCO.

Records to be kept by a Communications Service Provider

6.7 To assist the Commissioner carry out his statutory function in relation to Chapter II, CSPs should maintain a record of the disclosures it has made or been required to make. This record should be available to the Commissioner and his inspectors to enable comparative scrutiny of the records kept by public authorities. Guidance on the maintenance of records by CSPs may be issued by or sought from IOCCO.

6.8 The records to be kept by a CSP, in respect of each notice or authorisation, should include;

- the name of the public authority;

- the URN of the notice or authorisation;

- the date the notice was served upon the CSP, the authorisation disclosed to the CSP;

- a description of any communications data required where no disclosure took place or could have taken place, and

- the date when the communications data was made available to the public authority or, where secure systems are provided by the CSP, the date when the acquisition and disclosure of communications data was undertaken.

Errors

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

6.10 An error can only occur after a designated person:

- has granted an authorisation and the acquisition of data has been initiated, or
- has given notice and the notice has been served on a CSP in writing, electronically or orally.

6.11 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.

6.12 Where any error occurs, in the grant of an authorisation, the giving of a notice or as a consequence of any authorised conduct or any conduct undertaken to comply with a notice, a record should be kept.

6.13 Where communications data is acquired or disclosed wrongly a report must be made to the Commissioner ("reportable error"). Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error.

6.14 In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ("recordable error"). These records must be available for inspection by the Commissioner.

6.15 This section of the code cannot provide an exhaustive list of possible causes of reportable or recordable errors. Examples can 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

- disclosure of the wrong data by a CSP when complying with a notice;

- acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation;

Recordable errors

- a notice given which is impossible for a CSP to comply with and an attempt to impose the requirement has been undertaken by the public authority;

- 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[79], or data for which the requirement to acquire or obtain it is known to be no longer valid;

- failure to serve written notice (or where appropriate an authorisation) upon a CSP within one working day of urgent oral notice being given or an urgent oral authorisation granted.

6.16 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.

6.17 When a reportable error has been made the public authority which made the error, or established that the error had been made, must establish the facts and report the error to the authority's senior responsible officer and then to the IOCCO, in written or electronic form, within no more than five working days of the error being discovered. All errors should be reported as they arise. If the report relates to an error made by a CSP the public authority should also inform the CSP of the report in written or electronic form. This will enable the CSP to investigate the cause or causes of the reported error.

[79] 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.

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

6.19 Where a CSP discloses communications data in error it must report each error to the IOCCO within no more than five working days of the error being discovered. It is appropriate for a person holding a suitably senior position within a CSP to do so, identifying the error by reference to the public authority's unique reference number and providing an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. Errors by service providers could include responding to a notice by disclosing incorrect data or by disclosing the required data to the wrong public authority.

6.20 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.

6.21 Where material is disclosed by a CSP in error which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, that material and any copy of it should be destroyed as soon as the report to the Commissioner has been made.

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

Excess Data

6.23 Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority.

6.24 Where a public authority is bound by the 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 notice or 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.

6.25 If having reviewed the excess data it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The designated person 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.

DATA PROTECTION SAFEGUARDS

7.1 Communications data acquired or obtained under the provisions of the Act, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the Data Protection Act 1998 ('the DPA')[80] and its data protection principles must be adhered to.

7.2 Communications data ('related 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 conformity with the duty imposed upon him by the Act.

Disclosure of communications data and subject access rights

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

7.4 There is no provision in the Act preventing CSPs from informing individuals about whom they have been required by notice to disclose communications data in response to a Subject Access Request made under section 7 of the DPA. However a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA.

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

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

[80] Guidance is available from *www.dca.gov.uk/foi/datprot.htm* or *www.informationcommissioner.gov.uk*

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

7.8 Where a CSP is uncertain whether disclosure of the fact of a notice would be likely to prejudice an investigation or operation, it should approach the SPoC of the public authority which gave the notice – and do so in good time to respond to the subject access request. The SPoC can make enquiries within the public authority to determine whether disclosure of the fact of the notice would likely be prejudicial to the matters in section 29.[81]

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

7.10 CSPs should keep a record of the steps they have taken in determining whether disclosure of the fact of a notice would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police.

Acquisition of communication data on behalf of overseas authorities

7.11 Whilst 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.

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

7.12 There are two methods by which communications data, whether obtained under the Act or not, can be acquired and disclosed to overseas public authorities:[82]

- Judicial co-operation
- Non-judicial co-operation

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

Judicial co-operation

7.13 If the United Kingdom receives a formal request from an overseas court or other prosecuting authority that appears to have a function of making requests for legal assistance, the Secretary of State (in Scotland the Lord Advocate) will consider the request under the Crime (International Co-operation) Act 2003. In order to assist he must be satisfied that the request is made in connection with criminal proceedings or a criminal investigation being carried on outside the United Kingdom.

7.14 If such a request is accepted, that request will be passed to a nominated court in the United Kingdom. That court may make an order requiring a CSP to disclose the relevant information to the court for onward transmission to the overseas authority.

Non-judicial co-operation

7.15 Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries. These can include requests for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such a request the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Chapter II of Part I of the Act.

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

7.16 The United Kingdom public authority must be satisfied that the request 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

7.17 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.[83] Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

7.18 If the proposed transfer of data is to an authority within the European Union that authority will be bound by the European Data Protection Directive (95/46/EC) and its national data protection legislation. Any data disclosed will be protected there without need for additional safeguards.

7.19 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, including Canada and Switzerland, have laws providing an adequate level of protection where data can be transferred without need for further safeguards.

7.20 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. If necessary the Information Commissioner can give guidance.

[83] The eighth data protection principle is: 'Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.' (Paragraph 8, Schedule 1, DPA 1998)

7.21 The DPA recognises that it will not always be possible to ensure adequate data protection in countries outside of the European Union and the European Economic Area, and there are exemptions to the principle, for example if the transfer of data is necessary for reasons of 'substantial public interest'[84]. There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data. That is a decision that can only be taken by the public authority holding the data on a case by case basis.

[84] Paragraph 4, Schedule 4, DPA 1998

OVERSIGHT

8.1 The Act provides for an Interception of Communications Commissioner ('the Commissioner') whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter II of Part I of the Act. The Commissioner is supported by his inspectors who work from the Interception of Communications Commissioner's Office (IOCCO).

8.2 This code does not cover the exercise of the Commissioner's functions. It is the duty of any person who uses the powers conferred by Chapter II, or on whom duties are conferred, to comply with any request made by the Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.

8.3 Should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the Act in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal.

8.4 Reports made by the Commissioner concerning the inspection of public authorities and their exercise and performance of powers under Chapter II may be made available by the Commissioner to the Home Office to promulgate good practice and help identify training requirements within public authorities and CSPs.

8.5 Subject to the approval of the Commissioner public authorities may publish their inspection reports, in full or in summary, to demonstrate both the oversight to which they are subject and their compliance with Chapter II of the Act and this code. Approval should be sought on a case by case basis at least 10 working days prior to intended publication, stating whether the report is to be published in full, and if not stating which parts are to be published or how it is to be summarised.

COMPLAINTS

9.1 The Act established an independent Tribunal ('the Investigatory Powers Tribunal'). The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data under the Act.

9.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SW 1H 9ZQ

☎ 020 7035 3711