Home Office

Communications Data

Code of Practice

[Draft for consultation]

Communications Data

Code of Practice

[Month Year]

This publication is available at www.gov.uk/government/publications

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

ISBN XXXXXXXXX

.

Contents

Section 1

Introduction

1 Introduction

1.1 This Code of Practice ('the Code') relates to the exercise of functions conferred by virtue of Part 3 of the Investigatory Powers Act 2016 ('the Act'), as amended by the Investigatory Powers Amendment Act ('IP(A)A') 2024. Section 2 of this Code provides guidance on the procedures to be followed when acquisition of Communications Data ('CD') takes place under the provisions in Part 3 of the Act ('Part 3'). The previous section 3 of this Code provided guidance on the procedures to be followed when CD is retained under Part 4 of the Act ('Part 4') and is now included in the Notices Code of Practice.

1.2 This Code is applicable to relevant public authorities within the meaning of the Act and to telecommunications operators ('TO') and postal operators ('PO') which are defined under section 261 and section 262. The relevant public authorities are those public authorities that can acquire CD and are set out in Schedule 4 to the Act and local authorities listed in section 86 of the Act, by virtue of section 73(1).

1.3 The Act is designed to provide protections for CD relating to an individual by ensuring that public authority access to such material is tightly managed.

1.4 The default position is that an authority under Part 3 of the Act (or other Parts of the Act), or other judicial authority, should ordinarily be in place to enable disclosure, by compulsion, of CD from a TO.

1.5 There are limited exceptions to this position, and these are laid out in sections 11 and 12 of the Act.

Section 11

1.6 Section 11 of the Act states that if a person in a public authority knowingly or recklessly obtains CD from a telecommunications or postal operator without lawful authority, that person is guilty of an offence. Section 11 (3A) inserted by the IP(A)A, gives a number of examples of what constitutes 'lawful authority'. A Part 3 CD authorisation itself provides lawful authority to obtain CD, and in many situations using the Act to obtain CD will be the appropriate route. Public authorities should be aware that situations may arise where there are a number of possible lawful authorities available to obtain CD. This Code cannot account for all eventualities, but in these situations public authorities must be aware of their legal obligations, act responsibly and take great care to ensure that they obtain CD in the most appropriate way.

1.7 Public authorities should be aware that conscious and deliberate decisions to lawfully obtain CD outside of an IPA Part 3 authorisation are likely to be closely scrutinised by the IPC. Public authorities should be prepared to justify any such decisions. The IPC must keep under review functions relating to the acquisition or retention of CD that are exercisable under the Act, so may need to investigate, for example, any acquisition of CD suspected of being deliberately designed to avoid appropriate safeguards.

1.8 Where TOs make a lawful (e.g. UK General Data Protection Regulation ('GDPR') compliant) voluntary disclosure in response to a request from a public authority, the public authority will have lawful authority to acquire this CD.

1.9 Amendments to the Act made by the Investigatory Powers (Amendment) Act 2024 make clear that the offence of unlawfully obtaining CD applies only where the TO disclosing the CD is one which is not wholly or mainly funded out of public funds.

1.10 Therefore, wholly or mainly publicly funded bodies which acquire CD from another wholly or mainly publicly funded body which is also a TO under the Act, are excluded from the section 11 offence. However, such public authorities will still want to ensure, as a matter of good practice, that they have lawful authority to acquire that CD from another public body. If the acquiring public authority is seeking to rely on a supervisory or regulatory power to acquire the CD, they should note any limitations placed on the exercise of that power by s12 of the Act. This limitation is that the compulsion power is not available if it is being exercised for the purpose of pursuing a criminal investigation or prosecution. See paragraph 1.13.

1.11 The amendment to section 11 also provides examples, in a non-exhaustive list, of cases where a relevant person has lawful authority to obtain CD from a TO or PO. These include:

(i) where the relevant person's obtaining of the CD is lawful for all purposes in accordance with section 81(1);

(ii) any other case where the relevant person obtains the CD in the exercise of a statutory power of the relevant public authority;

(iii) where the operator lawfully provides the CD to the relevant person otherwise than pursuant to the exercise of a statutory power of the relevant public authority (whether or not in the exercise of a statutory power to disclose);

(iv) where the CD is obtained in accordance with a court order or other judicial authorisation;

(v) where the CD had been published and is publicly available before the relevant person obtained it; and

(vi) where the CD is obtained by the relevant person for the purpose of enabling, or facilitating, the making of a response to a call made to the emergency services.

1.12 The example at '(ii)' above is further qualified by section 12 of the Act. Where CD could be acquired through a Part 3 IPA authorisation but a public authority judge that it is more appropriate to use another lawful authority, the IPC may, as part of their oversight of the regime, require further justification and evidence of the decision-making process if, for example, it transpires that acquisition of CD has been deliberately designed to avoid appropriate safeguards.

Section 12

1.13 Section 12 of the Act (with Schedule 2) abolishes or amends other information gathering powers in law which provided for access to CD without appropriate safeguards. Accordingly, relevant public authorities for the purposes of Part 3 should not use other (non-IPA) statutory powers to require the disclosure of CD from a PO or TO unless that power:

(i) is authorised by a warrant or order issued by a person holding judicial office;

(ii) is exercised for regulatory or supervisory purposes and is not being exercised in the course of a criminal investigation; or

(iii) deals with TOs, POs, or a class of such operators and can be used either:

- in connection with the regulation of TOs, telecommunications services or telecommunication systems, or POs or services; or
- to acquire CD relating to postal items crossing the United Kingdom border.

Examples of lawful authority could include

1.14 Section 12 of the Act prohibits the use of general information gathering powers to require the disclosure of CD *except* where that general information gathering power is a 'regulatory or supervisory' power which is being exercised otherwise than in the course of a criminal investigation. Section 12 of the Act also does not prohibit any investigative enquiry requests such as with asset recovery not directly associated with the conduct of a criminal investigation and where no statutory power is being exercised.

1.15 A '**criminal investigation**' means an investigation of any alleged or suspected criminal conduct or to establish whether such conduct has taken place. Section 12(2C) of the Act outlines key definitions.

1.16 A general information gathering power, which is a regulatory or supervisory power, will be treated as 'not being in the course of a criminal investigation' for example if, at the time of the exercise of the power, the investigation is being conducted with a view to seeking a civil penalty, not a criminal conviction.

1.17 Section 12(6) of the Act states that a "regulatory or supervisory power" is a power to obtain information or documents which is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000 and is exercised in connection with:

(i) the regulation of persons or activities[1];

(ii) the checking or monitoring of compliance with requirements, prohibitions or standards imposed by or under an enactment; or

(iii) enforcement of any requirement or prohibition imposed by or under an enactment.

1.18 It is recognised that, on occasion, it may be necessary for a matter originally intended for civil resolution to move to criminal prosecution. The point at which a decision is made to move from a civil to criminal process may come *after* the original CD has been deleted by the TO. In these circumstances there was a lawful basis for the acquisition of the CD and a public authority does not need to re-obtain

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

that CD using an IPA Part 3 authorisation. The same applies for when the CD has not been deleted by the TO in that the public authority does not need to re-obtain that CD. However, a public authority must when seeking to acquire additional CD in support of an investigation (that has become a criminal investigation) seek an IPA authorisation or the most appropriate lawful authority. It is therefore not intended to prevent the use of CD, acquired using such general information gathering powers, from being later used in support of a criminal prosecution. Matters of admissibility of evidence should be left for the presiding court to determine.

1.19 Public authorities, who straddle both civil and criminal investigations may start a preliminary investigation which could remain a regulatory investigation or could turn into a criminal investigation. In such circumstances, where a public authority wishes to move from a civil to criminal resolution, it should have in place clear internal policy and operating procedures for managing such circumstances to give practical effect to paragraph 1.18. Public authorities' internal policy and procedures should promote sufficient record keeping during the acquisition process enabling an independent reviewer, with no prior knowledge of the case, to follow the developing circumstances and reach a similar conclusion regarding criminal escalation at broadly the same point in the enquiry.

1.20 Matters moving from initial civil compliance action to a criminal prosecution will be closely scrutinised by the Investigatory Powers Commissioner's Office ('IPCO'), during inspection of an organisation that conducts both criminal investigations and other civil compliance activity. This will provide the necessary independent oversight to ensure that the use of CD in criminal investigations is both lawful and proportionate in all circumstances. Public Authorities who seek to use CD, originally acquired using 'regulatory or supervisory' information gathering powers, should maintain an accurate and complete record of such instances. This should be made available to IPCO upon request, for example during an inspection.

1.21 Where a criminal prosecution is sought from the outset, relevant authorities with regulatory or supervisory functions must continue to use a Part 3 authorisation to gather CD or an appropriate lawful route set out in the Act.

1.22 Only public authorities specified in Schedule 4 or Schedule 2A of the Act may avail themselves of these regulatory or supervisory information gathering powers in respect of CD acquisition.

General principles

1.23 This Code should be readily available to members of a relevant public authority involved in the acquisition of CD under the Act, and to TOs and POs involved in the retention of CD and/or its disclosure to public authorities under the Act.

1.24 The Act provides that persons exercising any functions to which this Code relates must have regard to the Code when carrying out these functions. Failure to comply with the Code does not, of itself, make a person liable to criminal or civil proceedings but could assist a criminal or civil proceeding.

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

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

1.27 The exercise of powers and duties under Part 3 of the Act and this Code are kept under review by the IPC appointed under section 227 of the Act and by the Judicial Commissioners and inspectors.

1.28 The Home Office may issue further advice directly to public authorities, TOs and POs as necessary.

1.29 Although most of the Act has extra-territorial application, this Code extends to the United Kingdom only.

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

2 Scope and definitions

Overview

This chapter sets out guidance on and examples for the application of key definitions under the Act. It provides an overview of what constitutes a telecommunication operator and postal operator under section 261 and 262 and provides guidance for public authorities who are uncertain whether the data they seek to obtain fits the parameters of CD.

Telecommunications and postal definitions

2.1 A **telecommunications operator** ('TO') is a person[2] who:

- offers or provides a telecommunications service to persons in the UK;
- controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK; or
- controls or provides a telecommunication system which is not (wholly or partly) in, or controlled from, the UK and is used by another person to offer or provide a telecommunications service to persons in the UK.

2.2 This definition of a telecommunications operator makes clear that a UK nexus is required.

2.3 A TO will also include an application and website provider, but only in so far as they provide a telecommunications service.

2.4 A postal operator ('PO') is a person providing a postal service to a person in the UK. Section 262 of the Act defines 'postal service' to mean any service which consists in one or more of the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items and which has as its main purpose or one of its main purposes, the transmission of postal items from place to place.

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

2.6 The Act makes clear that any service which consists in, or includes, facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunication system is included within the meaning of 'telecommunications service'. Internet based services such as web-

[2] The term 'person' in this Code is the legal definition of 'person' which are entities that the law recognises as having certain rights and responsibilities, even though they are not living, breathing individuals. These can include corporations, partnerships, trusts, and government agencies.

based email, messaging applications and cloud-based services are covered by this definition.

2.7 The definition of TOs is intentionally broad. TOs may provide applications, websites, or some interface with the internet that facilitates electronic signals being sent between persons or things. The TO operation may be a small or a large part of their overall operations.

2.8 TOs include any website owner. The provision of the website is a telecommunications service by itself. It does not need to include any chat function. A website is also hosted on part of a telecommunications system i.e., a server. For the avoidance of doubt specific examples are included in the list below. This list is not exhaustive:

- providers of public telephony services
- Internet service providers
- the provider of any app that interfaces with the Internet
- Webmail providers
- online marketplaces
- streaming platforms
- social media platforms
- online dating sites
- online gaming companies and platforms
- online betting and casinos
- taxi companies (a taxi company with no online presence is not a TO as defined in the Act)
- providers of telecommunications services to SIMs embedded in vehicles
- food delivery services
- video conferencing and VoIP providers (voice-over internet protocol)
- Cloud providers
- instant messaging apps
- banks with an online presence and digital banking system
- online payment processors
- top up services
- government departments and public sector organisations subject to Crown immunity. [Note a TO does not need a CD authorisation to exploit/query its own CD, but one public authority may wish to obtain a CD authorisation if it is asking another public authority for CD that the second public authority is holding as a result of its operation as a TO. The acquisition of CD by a public authority from a publicly funded body which is a TO under the Act, is excluded from the section 11 offence. Refer to paragraph 1.9-1.10.] For additional examples please refer to Annex C.

2.9 The following paragraphs are intended to provide guidance for such circumstances. For additional guidance please refer to the flow chart at Annex B.

2.10 When information is sought from a person, consideration of the above paragraphs will be necessary, and the following scenarios will support public authorities in making the appropriate decision. These steps involve ensuring a Communications Data Single Point of Contact (‘CD SPoC’) is used. The CD SPoC maintains the relationships between TOs, POs and public authorities. CD SPoC may wish to speak to the operators to determine whether what is being sought is CD- see paragraph 5.4.

A person that solely provides a telecommunications service

2.11 Where information is sought from an operator who solely provides a telecommunications service then the data, for example the IP address will usually be CD and appropriate lawful authority will be required. If the public authority is unsure whether the information that is sought is CD, then a CD SPoC should be consulted if the acquisition is in support of a criminal investigation.

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

2.12 Where the information is sought from a person for which the telecommunications service is only a limited part of their offering, careful consideration will be required to determine whether an authorisation under Part 3 is required. While most information sought from such companies will not be CD, if the information that is sought would be CD in some contexts (e.g., telephone numbers or Internet Protocol ('IP') addresses) the public authority will need to consider whether the data is held in relation to the telecommunications service that the person operates or only available from a telecommunication system. If the data is held in respect of the telecommunications service or only available from a telecommunication system, then an appropriate authorisation will be required and the steps in this Code should be followed. Some companies will operate multiple distinct telecommunications services (e.g., an online dating service may operate a telecommunication system that allows customers to communicate with each other). They may also operate a telecommunication system in the form of a server that logs users to the site. If the public authority is unsure how the information is held then a CD SPoC should be consulted. Support and guidance for CD SPoCs can be found at paragraph 2.104.

2.13 If the information sought would be considered CD in some contexts e.g., because it is linked to a specific point in time or was logged automatically by a system or is relevant subscriber data under section 261(5A), then the request should be considered as an application for CD and will require a lawful authority for its disclosure.

For example:

Data Request	Request for CD?	Part 3 authorisation or other lawful authority for CD disclosure required?	Explanation
Individual's IP address when they registered for or last used an online marketplace.	✓	✓	This particular data is likely to only be held in respect of access to a telecommunications service or only available from a telecommunication system. This data is often logged automatically by the online market-place's telecommunication system when the service is used.

Where the CD is not explicitly requested

2.14 It is possible a person, such as with an online marketplace, may disclose data that would otherwise be CD in response to a request for the account information of a customer where CD is not explicitly being sought e.g., if the person decided to proactively access their servers to identify all IP addresses and times the customer had used their account and to disclose that information. There is no

breach of the Act in such circumstances because this CD was not requested, and it should be assumed that for business purposes data across telecommunication and non-telecommunication services is co-located. The data has been voluntarily disclosed by the person under data protection legislation which provides lawful authority for its disclosure. Where such data is disclosed by the person, it is good practice for the person within the requesting public authority who received the data to inform their CD SPoC so that the CD SPoC will be able to advise future applicants on how that person handles its data.

2.15 Where a relevant public authority wishes to acquire data that is both CD and other information, they will need to ensure they have lawful authority for both types of acquisition. Refer to Chapter 14 for the definition of lawful authority.

Other types of telecommunications operators

2.16 TOs may also include those persons who provide access to communications services that are secondary to the provision of another service, for example, in commercial premises (e.g., hotels) or public premises (e.g., airport lounges or public transport). Such telecommunications services may be provided by the overall service provider or by another TO as a partner or on their behalf. In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider (e.g., the hotel, restaurant, university, library, or airport lounges, or where there are security implications in doing so), the data may be sought from the TO which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of CD from such organisations; for example, where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room.

2.17 TOs may also include **financial institutions** in relation to some of the products, goods, and services they may offer. Financial Institutions may have statutory reporting requirements and/or obligations to disclose certain types of data (e.g., tax data, Financial Conduct Authority returns, money laundering or suspicious activity reports). Financial Institutions should refer to the relevant guidance in respect of these reporting obligations.

2.18 An IPA authority is only available for payment data (bank, card number, account holder, account holder address) relating to the provision of a telecommunications service or the use of the telecommunications service or system. A payment relating to a non-telecommunications service (e.g. a betting service) or a real-world service (e.g. taxi) will not be CD.

2.19 If the payment is for multiple services, so it covers the telecommunications service, but also some additional benefits (which might be real-world), then the payment data will be CD. Although payment data for non-telecommunications services and real-world services is not CD, the transaction or communication between the service provider and the customer can still generate CD by way of events data (time, IP address, MAC address etc) for which a CD authorisation is available.

2.20 For online banking the CD can be generated when transactions are undertaken, but the content of the banking transaction is not CD (to whom money paid, amount etc.). Refer to Annex C for additional examples.

Postal operator

2.21 Section 262 of the Act defines '**postal service**' to mean any service which consists in one or more of the collection, sorting, conveyance, distribution and delivery (whether in the UK or elsewhere) of postal items and which is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to transmit postal items from place to place.

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

2.23 A person, due to their services offered, can fall into both categories as a TO (section 261) and a PO (section 262), (e.g., where a PO offers online platforms and applications allowing communication between the postal recipient and the operator). If the person holds telecommunications data, they do so as a TO and not a PO.

Composition of communications

2.24 For the purposes of the Act communications may comprise two broad categories of data: **systems data** and **content**. Some communications may consist entirely of systems data and will not therefore contain any content. Section 261(6)(b) makes clear that anything which is systems data is, by definition, not content. Systems data includes CD as defined in section 261(5).

2.25 Additionally, when permitted by the Act, certain data may also be separated from the remainder of a communication in circumstances where, if it were so separated, it would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, this is **identifying data**. Systems data and identifying data may be obtained by interception or equipment interference warrants under Parts 2 and 5, and Chapters 1 and 3 of Part 6 of the Act. Further details on systems and identifying data can be found in the Interception of Communications and the Equipment Interference Codes of Practice.

2.26 CD is a subset of systems data, see section 263(4) of the IPA. The Act is clear that, even though systems data cannot be content, CD is limited to data which does not reveal anything of what might reasonably be considered to be the meaning of the communication (but any meaning arising from the fact of the communication or transmission of the communication is not content). That is, any systems data which would, in the absence of section 261(6)(b), be content, cannot be CD. The Investigatory Powers (Amendment) Act 2024 amended section 261 of the Act with the effect that 'relevant subscriber data' is excluded from the content carve out. "**Relevant subscriber data**" is data (other than data comprised in a recording of speech) which is about an entity to which a telecommunication service is provided and constitutes any of the content of a communication made for the purpose of initiating or maintaining an entity's access to a telecommunication service (e.g., subscriber data passed in an online form, refer to Annex C for more examples).

2.27 When seeking subscriber data, the applicant/CD SPoC needs to explain how the account subscriber data being sought relates to the provision or use of that part of the business that is operating as a TO. One way of thinking about whether data relates to the provision of the telecommunications service is to consider whether

the TO would still be able to provide the customer with the telecommunications service or system without this data. If not, or if the telecommunication service would not function in the same way, then the account subscriber data probably does relate to the provision of the service and therefore is CD. Whether the account data relates to the use of the service will be a question of fact. If it does, then it will probably be CD. For example, where the TO is:

- exclusively a TO, it is likely that **all** the registration data will be covered under IPA.
- partially a TO, it is likely that only **some** of the registration data will be covered under IPA.

2.28 For example, an auction house that additionally provides for online bidding which is only in part a TO, the name and email address given as part of the registration for the online bidding function will be CD. Payment details (bank, card number, account holder, account holder address) will not normally be CD *unless payment details are required in order to access the service in the first place.* Additional profile details, payment details relating to purchase of goods etc. will not be CD. A profile photograph or picture will not usually be CD because it does not normally relate to the provision or use of the telecommunications service unless it is a mandatory feature required as part of subscriber and account data in order to access the service (see Annex B and C).

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

2.30 CD authorisations may authorise limited interference with equipment by a TO where that is done solely to enable or facilitate the acquisition of CD from the network for the purposes of identifying an entity as well as information about their previous or current location.

2.31 Cell site data about a communication device will be CD because it is information identifying the apparatus through which a communication is, has, or may be made. Location tracking data from a vehicle's on-board tracking device, which is derived only from cell site reference data via a SIM card, is CD for the same reason. IP addresses and Wi-Fi factors such as Basic Service Set Identifier ('BSSID'), which can be used independently to identify a physical address for the IP address subscriber and the WI-FI access point respectively, are CD. Location data derived from the 'location service' within a device, blended from different data sources to generate a location to support, for example, travel and mapping applications, will not usually be CD because that information is not required for the provision of the underlying telecommunications service. Such data sources might include Global Positioning System ('GPS'), Assisted Global Positioning System ('AGPS'), Wi-Fi or IP address. Any systems data that reveals the current or previous location of an entity, and is data required for the purpose of initiating or maintaining access to a telecommunications service, will be CD. Please see provision in section 261 as amended by the Investigatory Powers (Amendment) Act 2024.

Communications Data ('CD')

2.32 The term 'communications data' includes the 'who', 'when', 'where', and 'how' of a communication (but not the 'content' - e.g., what was said or written. However, there is a subset of "content" which can be considered to be CD- see section 261(5) of the Act and paragraph 2.69 for the definition of 'content').

2.33 It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning (set out at section 261(6)(a) of the Act), of the communication (unless the content falls within the small subset that may be CD, referred to above).

2.34 CD can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access and relevant subscriber data, internet telephony, instant messaging and the use of applications and includes postal services. This Code only covers CD relating to the provision of a telecommunications service or system and the use of a telecommunications service or telecommunications system, and a postal service where its main purpose (or one of its main purposes) is to make available or facilitate the transmission of postal items containing communications. Data that is out of scope may be acquired by other alternative legislation.

2.35 CD is generated, held or obtained in the provision, delivery and maintenance of communications services (e.g., postal services or telecommunications services).

2.36 A **CD product** is a defined data product containing a certain set of fields. A product can be selected based upon a certain set of query terms which the TO can use to select the particular product of interest e.g., the Mobile Station International Subscriber Directory Number ('MSISDN'), International Mobile Equipment Identity ('IMEI') or account ID for the customer along with time-parameters (e.g., a Simple Query). CD Products could be the customer record for an identified customer (e.g., entity data), the in and out call data for a customer over a period of time, the cell-site derived location data for a customer, or the Internet Connection Records for a customer (e.g., events data). Conversely, a Compound Query, can (but does not need to) provide additional instructions for selecting certain records and fields from within a product (and could be applied to entity or events data but more likely events data). Refer to paragraph 5.16 and 5.17.

Telecommunications definitions

2.37 CD is made up of entity and events data (see paragraphs 2.49 onwards for more detail on these terms) in relation to TOs' services and systems includes data held or obtainable by a TO or PO or which is available directly from a telecommunication system and comprises of four elements:

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

2.38 This data includes information about any person or entity to whom a service is provided, whether a subscriber or guest user, and whether they have ever used that service (e.g., information about the person associated with an email address

even if that email address has not been used since its creation). This may include names and contact details of subscribers.

2.39 An entity (see below for further details) can also include an account holder and/or devices. This data would cover information about the devices used by a customer and the services provided by the TO (to which the user of the devices subscribes).

2.40 Importantly this data is limited to data held or obtained by the TO in relation to the provision of a telecommunications service. It does not include data which may be held about a customer by a TO more generally which is not related to the provision of a telecommunications service. For example, Know Your Customer ('KYC') information held by a financial institution would only be CD if it related directly to the provision of a telecommunications service and was obtained specifically for this purpose, or otherwise met one of the other limbs for CD detailed below. This data includes any information that is necessary to get a communication from its source to its destination, such as the dialled telephone number or Internet Protocol ('IP') address. It includes data which:

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

Data comprised in, included as part of, attached to or logically associated with a communication for the purposes of a telecommunication system by means of which the communication is or may be transmitted

2.41 This element of the CD definition also includes data held, or capable of being obtained, by the TO which is logically associated with a communication for the purposes of the telecommunication system by which the communication is being, or may be, transmitted. In practice this will often mean any data which is used to route or transmit a communication which the TO holds or could obtain, for example from the network.

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

2.43 Information falling within this section of the definition of CD can be obtained directly from a telecommunication system by a public authority, see section 261(5)(b) of the Act.

Data which relates to the use of a telecommunications service or system

2.44 This element includes other entity or events data held by a TO about the use of the service such as information that the provider holds for billing/charging purposes or business records where appropriate.

2.45 For example, for a social networking provider, data such as the status of the account and the date a person registered with the service would all be CD as they relate to the use of the service.

2.46 However, other data held by the provider about a customer which does not relate to the use of the telecommunications service, including contact details for the customer which will likely be associated with the *provision* of the service. Additionally, personal information such as political or religious interests included in profile information, is not immediately within scope of the definition of CD unless it is mandatory registration information then it will be CD because it relates to the provision of the service. (See paragraph 2.28 for further examples.)

Data which is about the architecture of a telecommunication system and not about a specific person

2.47 The definition of CD additionally includes data held by a TO about the architecture of the telecommunication system (sometimes referred to as '**reference data**'), e.g., this may include the location of mobile phone masts and cell sites or Wi-Fi access points. This information itself does not contain any information relating to specific persons and its acquisition alone does not interfere with the privacy of any customers therefore this does not require an IPA Part 3 application. However, this data is often necessary for the public authority to interpret the data received in relation to specific communications or users of a service. Such data may be commercially sensitive, and an authorisation can be sought by a public authority seeking to obtain this data from a TO where the TO requires it.

2.48 See paragraph 2.73 for guidance on when data was inputted online or in-person.

Entity and Events Data

2.49 All CD held by a TO or obtainable from a telecommunication system falls into two categories:

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

2.50 The authorisation levels required to access CD reflect the fact that events data contains more intrusive CD (e.g., information on who has been in communication with whom, a person's location when their mobile device connects to the network and internet connection records) than entity data. The rank of the designated senior officer that can authorise acquisition of data reflects the differing levels of intrusiveness of the data. For example, in certain circumstances, the police can authorise access to entity data at Inspector level, but events data is authorised at Superintendent level. Additionally, entity data can be obtained in a wider range of crime types than events data. An application for CD must always be categorised at the highest level of intrusion, e.g., as an application for events data wherever any events data is requested.

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

2.52 Where a public authority provides events data to a TO as part of a request for entity data then the TO may disclose that events data in the response to the entity data authorisation. Taking the example in paragraph 2.45, the TO could include the time and date of the communication as part of the response without the need for it to be authorised as an event. This is because the public authority, by providing the events data to the TO, has demonstrated they are already aware of the event and only intend to determine the entity involved in that event. By disclosing the events data, the TO would only be providing the public authority with information they already knew. Such disclosure is likely to occur where the TO discloses the full record from their systems.

Entity data

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

2.54 Examples of entity data include:

- 'subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments online or registration details relating to a telecommunications service or other relevant subscriber data;
- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes;
- online or registration details relating to a telecommunication service
- Vehicle Identification Numbers(s) ('VIN') when linked with a SIM card imbedded within a vehicle ('connected vehicle'). However, within this example, when the owner of the vehicle is a victim in a criminal investigation consent should be sought from the victim where appropriate to acquire the data;
- this includes Personal Unlocking Key ('PUK') 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.

2.55 Entity data can change over time. For example, if someone moves house the address held by a TO will be updated and changed. The fact of that is an attribute of the entity (the person) and not a communication event.

Passwords

2.56 Some TOs may choose to retain user passwords as 'clear text' for business purposes. In many cases a TO will retain a 'password hash' rather than the password itself. When a user enters the password to use a service it is encrypted, and the hash generated is checked against the hash already held by a TO meaning the operator never needs to retain the actual password. In this context passwords would constitute entity data. Any information, such as a password,

giving access to the content of any stored communications or access to the use of a communications service may only be sought under Part 3 of the Act from a TO in the following circumstances:

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

2.57 A CD authorisation cannot authorise a public authority to use a password obtained through that or another CD authorisation. If a public authority wishes to use a password obtained through a CD authorisation to access the content of either stored or live communications or any communications service it must, in accordance with section 6 of the Act, ensure that it has appropriate lawful authority.

Events data

2.58 Events data covers information about time-bound events taking place across a telecommunication system. Events data is limited to communication events describing the transmission of information between two or more entities over a telecommunications system. This will include information which identifies, or appears to identify, any person, apparatus or location to or from which a communication is transmitted. '**Apparatus'** is defined in section 263 of the Act to include "any equipment, machinery or device (whether physical or logical) and any wire or cable". It does not include non-communication activities such as a change in address or telephone number for a customer.

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

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

Postal definitions

2.60 A postal service is a service which involves one or more of the collection, sorting, conveyance, distribution and delivery of postal items and where its main purpose (or one of its main purposes) is to make available or facilitate the transmission of

postal items containing communications. CD, in relation to a postal service, is defined at section 262(3) of the Act and comprises three elements:

Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted

2.61 "Postal data" is defined in section 262(4) of the Act and includes specified categories of data written on the outside of a postal item. All information on the outside of a postal item concerning its postal routing is postal data (e.g., the address of the recipient, the sender and the post-mark).

2.62 Postal CD will include postal data which includes any information that identifies, or appears to identify, any person or location to or from which a communication is or may be transmitted and includes:

- anything written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item's postal routing, sender or recipient (e.g., address or markings);
- identification of the origin or source of a postal item;
- records of correspondence checks comprising details of data from postal items in transmission to a specific address;
- identification of the vehicle or device used in delivering a postal item (Personal details of the driver or courier responsible for delivering a postal item are not defined as CD under the IPA and it is not appropriate to use the IPA provisions to request and acquire this data from a PO);
- details of the time, date and location of delivery of a postal item. For example, this can include the geo-location data of the delivery location of the postal item;
- data which confirms the delivery of a postal item to its intended recipient. This can include recipient signatures or photographs of postal items at the delivery address where available; and
- online tracking of communications (including postal items and parcels).

Information about the use made by a person of a postal service

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

- time-bound information about the use made of services which the user is allocated, has selected or has subscribed to (or may have subscribed to) including for example the details of the redirection of a given postal item at a time and date to an alternative address, facility or other delivery point;
- the price paid to send an item and the postage class used;
- data describing the weight, dimensions or size of the postal item; and
- records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

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

2.64 This includes information about any person to whom a service is provided, whether a subscriber or guest user and whether or not they have ever then used that service. (E.g., this may include the name, street address, contact numbers and email addresses of those customers. It may also include information about

the person associated with a PO Box even if that PO Box address has never received any mail).

2.65 As with the telecommunications definitions this does not include data which may be held about a customer by a PO more generally which is not related to the postal service.

2.66 Examples of data under this element of the definition of postal CD include:

- information about the subscriber to a PO Box number or a postage paid impression used on bulk mailings;
- information about the provision to a subscriber or account holder of a permanent or semi-permanent forwarding redirection arrangement and to what forwarding addresses;
- information about the provision of other services to postal account holders, (e.g., of services designed to protect or hold postal items when the recipient is unable to take receipt); and
- subscribers' or account holders' account information, (including names, addresses, telephone numbers and emails addresses and billing including payment method(s) and details of payments) which is not within the first or second elements of postal CD.

2.67 Those public authorities that, under certain conditions, can authorise access to entity data at a lower level of seniority may also authorise access to this element of postal CD at the same level.

2.68 The provisions previously detailed at paragraphs 1.11-1.19 concerning regulatory or supervisory information gathering powers are affected, in relation to Border Force, by section 352 of the Finance (No. 2) Act 2023. That provision states that section 12(2) of the IPA does not apply to powers conferred by the customs and excise Acts (within the meaning of Customs and Excise Management Act 1979 ('CEMA')[3]. In so far as Border Force rely on any other powers to acquire CD, the paragraphs at 1.11-1.19 of this Code are likely to apply to Border Force in their regulation or supervision of fast parcel services concerning shipments to, from, or otherwise linked or associated with a given address, sender or receiver in respect of parcels suspected of containing illicit goods.

Content of a communication

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

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

[3] Changes made in the section 352 of the Finance (No.2) Act 2023 made it clear that HMRC's use of its statutory powers to require the disclosure of communications data for its civil functions to assess and collect tax due and to meet its obligations under international treaties, was not restricted by section 12 of the IPA 2016. The IP(A)A 2024 made similar changes to those made in section 352 of the Finance (No.2) Act and extended to all organisations listed within Schedules 2A and 4 of the IPA with supervisory and regulatory statutory powers.

a messaging application) that conveys substance or meaning. It is information which conveys that meaning that the Act defines as content.

2.71 When a communication is sent over a telecommunication system it can be carried by multiple operators. Each operator may need a different set of data in order to route the communication to its eventual destination. Where data attached to a communication is identified as CD it continues to be CD, even if certain providers have no reason to use this data (see paragraph 2.98 onwards). The definition of content ensures that the elements of a communication which are considered to be content do not change depending on which communication provider is carrying the communication.

2.72 There are two exceptions to the definition of "content" and one type of data that is excluded from the content "carve out". The exceptions are in 261(6)(a) and 261(6)(b) & exclusion is found in section 261(5A) & (5B)

2.73 The **exclusion from the content "carve out",** at section 261(5A) & (5B), is in the context of "relevant subscriber data" and was inserted into the IPA by the Investigatory Powers (Amendment) Act 2024. "Relevant subscriber data" means entity data, other than data comprised in a recording of speech, which constitutes any or all of the content of a communication made for the purpose of initiating or maintaining an entity's access to a telecommunication service and is about an entity to which that telecommunication service is, or is to be, provided. As an example, data submitted within an online form could be considered as providing the 'meaning' of a communication. Section 261(5A) makes clear this type of information is "relevant subscriber data" where it is for the purpose of initiating or maintaining access to a telecommunications service and is entity data and CD (see paragraph 2.26). For example, when seeking to identify the driver of a hire car, the driver's name and address details inputted via an online booking form will be CD and not content. In this example, the hire company is providing the telecommunications 'service' used to book the hire car and the data provided was for the purpose initiating or maintaining access to the telecommunications system through which the car could be booked. If the public authority is unsure whether the CD has been provided online or in-person to a company representative and entered into an electronic system manually, then they must apply for a Part 3 authorisation or utilise another appropriate lawful authority.

2.74 The **first exception to the meaning of "content",** at 261(6)(a), is any meaning that could be inferred from the fact of the communication. When a communication is sent, the simple fact of the communication may convey some meaning, (e.g. it can provide a link between persons or between a person and a service). This exception makes clear that any CD associated with the communication remains CD and the fact that some meaning can be inferred from it does not make it content.

2.75 The **second exception**, at 261(6)(b), makes clear that systems data (defined in section 263(4)) cannot be content.

Postal content

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

sender and the post-mark) is postal data and will not be content. In the context of postal communications secondary data is limited to system data. Further examples of CD may include messages written by the sender concerning the delivery aspects of the postal item e.g. where to leave a delivery including potential contact number or alternative address details.

Web browsing and communications data

2.77 Web browser software provides one way for users to access web content (although there are other commonly used mechanisms, such as dedicated applications). When using a browser to access the web, a user may enter a web address. These are also referred to as a Uniform Resource Locator ('URL').

2.78 In order to access a webpage over the internet, key parts of a URL are normally converted from the web address format with which we are familiar (e.g., http://www.example.com) to numeric IP addresses, for example, by means of the Domain Name system ('DNS') protocol.

2.79 URLs follow a standardised structure and will always contain:

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

2.80 In order for the process of gaining access to a web address to be completed an IP address is required; this may be derived from a fully qualified domain name ('FQDN').

2.81 Where a host identifier only provides a partially qualified domain name ('PQDN') the DNS process must generate a FQDN for the browser, or the communication will fail. Some web sites split their content across a number of servers. As the content is split across a number of servers, elements of the URL may be used to route the communication to the correct server.

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

2.83 Additionally, URLs may, (but do not always) contain:

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

2.84 The port and, where required to route a communication, the user info will be CD.

2.85 An authorisation under Part 3 of the Act or retention notice under Part 4 of the Act may only authorise the acquisition or retention of CD, and therefore can only cover those elements of a URL which constitute CD. However, where it is not possible to reliably separate non-CD data from a URL this would fall under the "**inextricably linked**" data provisions (see paragraph 5.23).

Relevant communications data

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

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

- the sender or recipient of a communication (whether or not a person) this can include phone numbers, email addresses, user identities and other information which can identify a customer such as names, addresses, account details and other contact information held as necessary for provision of the telecommunication service or use of the telecommunication service or system. In the context of internet access this can include source and destination IP addresses, port numbers and the relevant elements of URLs (See section on web browsing and CD at paragraphs 2.77-2.85);
- the time or duration of a communication. This can include the time and duration of phone calls, the time of emails, connections on the internet or internet access sessions;
- the type, method or pattern, or fact, of communication. This can include records showing the usage of a communication system;
- the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted. This can include the identities of mobile phone masts or Wi-Fi access points to which a device has connected; or
- the location of any such system (or any part of it). This can include the physical location of phones or other communication devices or the location of mobile phone masts or Wi-Fi access points to which they connect.

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

2.89 The data to be retained under a retention notice will be set out in the notice. A notice may provide for the retention of data that is necessary to enable the TO or PO to correlate the above data and disclose it when required to under Part 3 of the Act. This may include, but is not limited to, customer reference numbers.

2.90 Section 87(4) of the Act ensures that a retention notice must not require the retention of third-party data unless that data is, or can only be obtained by processing, an internet connection record (see below). Where the TO needs the data for the functioning of a telecommunication system or where the data is retained or used for any other purpose, it is not third-party data. Determining what is third party data and whether it can be separated from other data is complex and will require careful consideration on a case-by-case basis as part of the consultation before a retention notice is given. See paragraphs 2.98 to 2.103 for more information on third party data.

Internet connection records

2.91 An internet connection record ('ICR') is a record of an event held by a TO about the service to which a customer has connected on the internet. An ICR is CD which may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or program where that data is generated or processed by a TO in the process of supplying the telecommunications service to the sender of the communication. In many cases ICRs will be held by internet access providers, which are TOs providing access to the internet and can include a home broadband connection, mobile internet or publicly available Wi-Fi.

2.92 An ICR will only identify the service that a customer has been using. For example, many social networking apps on a device maintain persistent connections to a service. Even in this case the relevant ICR will signpost the service accessed by the device, enabling the public authority to make further enquiries of the social networking provider identified from an ICR.

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

- a customer account reference – this may be an account number or an identifier of the customer's device or internet connection;
- the source IP address and port;
- the destination IP address and port – this is the address to which the person or equipment is routed on the internet and could be considered as equivalent to a dialled telephone number. The port additionally provides an indication of the type of service (for example website, email server, file sharing service, etc.) although ports are often reused for different purposes; and
- the date/time of the start of the event and its end and/or its duration.

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

- the volume of data transferred in either, or both, directions;
- the name of the internet service or attributable server that has been connected to; and
- those elements of a URL which constitute CD (see paragraphs 2.77 to 2.85).

2.95 Where a data retention notice is considered, which would require a TO to retain ICRs, the specific data that an internet access provider may be required to retain will be discussed with the provider before the requirement is imposed (see the Notices Code of Practice).

2.96 The restriction on the retention of third-party data does not apply to ICRs.

2.97 ICRs can include connections which are made automatically by a person's browser, applications and/or other programs, or device. They are therefore not limited to human initiated events and will include machine to machine or machine to human initiated activity.

Third party data

2.98 Where a communication is sent there may be multiple providers involved in the delivery of the communication. Each provider may require different elements of CD to route the communication. E.g., when sending an email, there will be the email provider, the internet access provider for the sender and the internet access provider for the recipient. The email provider will require the email address to route the communication but neither internet access provider has any need to see nor access the entire email address in order to route the message to and from the sender's or recipient's mail servers.

2.99 Where one TO can see and/or access the CD in relation to applications or services running in the clear over their network, but that data is not needed by the system operator for the functioning of the system in relation to that communication, this is regarded as third party data. A TO is considered to process data if it specifically reviews an item of data in order to determine what action to take, or if it has a set of rules in place which determine how a communication should be routed depending on certain items of data.

2.100 If a TO or PO has no need of the data for the functioning of the system in relation to that communication but extracts and retains this data or generates a product from this data for their own business purposes (e.g., for network diagnostics), then it is no longer regarded as third-party data and this data could therefore be covered by a data retention notice. A CD authorisation may be given for the acquisition by a public authority of third-party data on a forward-looking basis where necessary and proportionate in relation to a specific investigation. A TO or PO need only obtain and disclose third party data where reasonably practicable to do so. Where such data is encrypted by the third-party a TO is under no obligation to decrypt such information.

2.101 Section 87(4) Investigatory Powers Act 2016, as amended by the Investigatory Powers (Amendment) Act 2024, makes clear that the restriction in ability for a Retention Notice to require retention of third-party data does not apply in relation to;

(i) data which is or can only be obtained by processing an internet connection record;
(ii) a relevant roaming service.

2.102 Section 4A defines a "relevant roaming service" as a telecommunications service provided by the system operator under an agreement with a TO outside the United Kingdom (the "non-UK operator") which facilitates the use by persons in the United Kingdom of the system operator's telecommunication system to access one or more telecommunications services of the non-UK operator.

2.103 A relevant roaming service exists where a UK TO has an international roaming agreement with an overseas TO ('OTO') which facilitates access to a telecommunications service or services provided by the OTO to one of its customers roaming in the UK. For example, where a person is using a SIM card or eSIM from an OTO to access the OTO's services while roaming on a UK mobile network. In these circumstances, the retention notice could cover retention of CD by the UK TO that relates to the calls and messaging that are handled by the OTO.

Guidance on definitions

2.104 Where an applicant is unsure of the category of data they are seeking (entity or events data) or what additional types of CD may be retained by a TO or PO for their own business use, the applicant should discuss this with their CD SPoC. If a CD SPoC or DSO wishes to find out more, they should consult the relevant TO or PO or contact the CD Knowledge and Engagement Team.

2.105 The Home Office may issue further guidance to TOs, POs or public authorities, on how the definitions in the Act apply.

Section 2
Communications data acquisition and disclosure

3 General extent of powers

Overview

This chapter sets out guidance for public authorities in their consideration of necessity, proportionality and seriousness prior to making a Part 3 authorisation.

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

3.2 Training should be made available to all those who participate in the acquisition and disclosure of CD. For law enforcement, both the College of Policing and a CD Professional Oversight Board established by the National Police Chiefs Council perform a role in relation to compliance training for relevant personnel who have responsibilities set out within legislation relating to the lawful acquisition of CD. All standards are set in accordance with legislation and codes of practice. Any training, advice and recommendations made by these bodies may be made available to all relevant public authorities.

Considerations regarding necessity

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

- in the interests of national security;
- for the applicable crime purpose;
- in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security;
- in the interests of public safety;
- for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- to assist investigations into alleged miscarriages of justice; or
- where a person ('P') has died or is unable to identify themselves because of a physical or mental condition to a) assist in identifying P, or b) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.

3.4 The applicable crime purpose will depend on whether the CD being sought is classified as entity data or events data. The definition of applicable crime purpose is found in section 60A(8) and repeated in sections 61(7A) and 61A(8). It means that, where the CD sought is wholly or partly events data, the purpose must be for "serious crime" as defined in section 86(2A). In any other case the CD must be for the purpose of preventing or detecting crime or of preventing disorder. Section 263(6) provides further clarity on what "detecting crime or serious crime" means.

3.5 For the purposes of Parts 3 and 4 of the Act "**serious crime**", defined in section 86(2A) of the Act, means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal (see section 263(1) of the Act, with paragraph 6 of

Schedule 9) ; any offence committed by a body corporate (a body corporate is an organisation such as a person or government that is considered to have its own legal rights and responsibilities) ; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

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

3.7 This does not prohibit data lawfully acquired under a Part 3 authorisation, or any other lawful authority, from subsequently being used to support civil or disciplinary action.

3.8 The statutory purpose 'in the interests of public safety' should be used by public authorities with functions to investigate specific and often specialised offences or conduct such as accident investigation or for example, a large-scale event that may cause injury to members of the public. Public safety should not be interpreted as for purposes relating to crime that impacts on the public, such as the sale of illegal drugs.

3.9 The statutory purpose 'for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health' can include those situations where, for example, there is serious concern for the welfare of a vulnerable person, for example, if such a person is missing.

3.10 The purposes for which individual public authorities are permitted to seek to acquire CD are set out in Schedule 4 to the Act (and for local authorities in section 73). The authorising individual (see paragraph 4.11) may only consider necessity on grounds open to the individual public authority and only in relation to matters that are the statutory or administrative function of the respective public authority.

3.11 Where an authorisation is granted under section 60A(1)(b)(ii) or 61(1)(b)(ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of CD, the authorising individual must be clear that it is also required for one of the specified purposes and the application is proportionate to what is sought to be achieved. There may be circumstances where it is appropriate to use a testing authorisation in respect of a real investigation. For example, if a TO or PO has started retaining a new data type a public authority will need to begin acquiring that data to test the reliability of the TO's or PO's retention systems. In such circumstances, it might be appropriate to authorise the testing in respect of a specific investigation so as not to unnecessarily infringe on the privacy of someone entirely unrelated to any investigation.

3.12 Before public authorities can acquire CD using an IPA Part 3, authorisation must be given by an authorising individual. An application for that authorisation must include an explanation of the necessity of the application.

3.13 Necessity should include an outline of why the data is required for the purposes of the investigation or operation. It should also include a short explanation of the investigation or operation, the person and the CD and how these three link

together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of CD is necessary for the statutory purpose specified.

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

- the event under investigation (e.g., a crime or vulnerable missing person), see paragraph 3.23;
- the person whose data is sought (e.g., a suspect, witness or missing person) and how they are linked to the event; and
- the CD sought, (e.g., a telephone number or IP address) and how this data is related to the person and the event.

Considerations regarding proportionality

3.15 When granting an authorisation, the authorising individual must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified CD and that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

3.16 As well as consideration of the rights of the individual whose data is to be acquired consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation.

3.17 Section 2 of the Act requires an authorising individual to have regard to the following when granting an authorisation to obtain CD:

- whether what is sought to be achieved could reasonably be achieved by other less intrusive means;
- whether the level of protection to be applied in relation to obtaining CD is higher because of the particular sensitivity of that information;
- the public interest in the integrity and security of telecommunication systems and postal services; and
- any other aspects of the public interest in the protection of privacy.

3.18 **Collateral intrusion** is the obtaining of any information relating to individuals other than the subject(s) of the investigation. The degree of collateral intrusion forms part of the proportionality considerations and becomes increasingly relevant when applying for events data.

3.19 Particular consideration must also be given, when relevant, to the right to freedom of expression and the need to protect the public interest in the confidentiality of sources of journalistic information through judicial approval of relevant applications. See section on applications for CD relating to determining or confirming the source of journalistic information beginning at paragraph 8.12 for further information and guidance.

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

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

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

3.23 The relevance of the data being sought should be explained as should any information that the applicant is aware of which might undermine the application. Matters of reputational risk and public confidence are not to be factored when addressing proportionality.

3.24 In cases where there has already been an application or applications for CD, but more CD is still required to achieve the same objective, the applicant should consider all CD that has previously been obtained to decide if it is proportionate to request further CD. Another request for CD may no longer be a proportionate interference with the rights of the subject or other individual and/or no longer be necessary to the investigation in the public interest. For example, where possible the applicant could explain within their subsequent applications why prior requests have failed to meet the operational objective.

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

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

3.27 An examination of the proportionality of the application should particularly include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation. Applications should take into account an individual's right to hold and express opinions which might be subjectively distasteful or offensive but fall short of meeting a criminal threshold.

3.28 When seeking CD, it is important to note that collateral intrusion occurs at the point of acquisition irrespective of any subsequent action. While the way CD is handled and analysed after acquisition may *mitigate* the impact of collateral intrusion, it does not affect its likelihood as it will already have taken place. Applications should include details of what collateral intrusion may occur and how the time periods requested may impact on the collateral intrusion. When collateral intrusion is likely to be more limited, such as when applying for entity data in relation to a person under criminal investigation, the absence of collateral intrusion should also be noted.

3.29 An application for the acquisition of CD should draw attention to any circumstances which give rise to significant collateral intrusion. In such cases it may be appropriate to utilise the request filter (see Chapter 11).

3.30 Applications for the acquisition of CD should include details of parameters that the TOs and POs themselves may be able to apply to the data to assist in reducing collateral intrusion. In some circumstances it will be possible for the operator in question to apply filtering themselves to the data to select only that data which is relevant to the investigative outcome sought. Where this is possible collateral intrusion will be reduced. This should be explained in the application, drawing attention to the parameters used and how these are designed to select only the

relevant data. The request filter (filtering arrangement) may be used in combination with this approach to keep the anticipated collateral intrusion to the minimum possible.

3.31 An examination of the proportionality of the application should also involve a consideration of possible unintended consequences and, when relevant, this should be noted. Unintended consequences are more likely in complicated requests for events data or in applications for the data of those in professions with duties of confidentiality. For example, if a journalist is a victim of crime, applications for events data related to that journalist's phone number as part of the criminal investigation may also return some phone numbers of that journalist's sources, with unintended impact on freedom of expression. Such an application may still be necessary and proportionate, but the risk of unintended consequences should be considered including the ways their impact will mitigated. The special considerations that arise in such cases are discussed further within paragraphs 8.8 to 8.37.

Considerations regarding seriousness

3.32 These considerations should be taken into account when applying for data for the statutory purpose of the prevention and detection of serious crime as defined in section 86(2A) of the Act.

3.33 As set out in paragraph 5.3, a public authority must clearly explain how they have considered the necessity and proportionality for acquiring CD within the CD application form. The public authority must also set out if the crime is sufficiently serious to justify the acquisition of such data.

3.34 Those involved in the acquisition of events data as CD should be clear that the serious crime threshold under section 86(2A) is an absolute minimum criteria. In practice, most offences for which CD is acquired will be significantly over this threshold. However, some offences that are significantly over the threshold, such as theft, will include particular crimes, such as an isolated case of minor shoplifting, which are highly unlikely to be sufficiently serious to necessitate the acquisition of CD.

3.35 For offences that meet the different (and higher) serious crime threshold for interception, equipment interference and bulk powers (set out in section 263(1) of the Act, and paragraph 6 of Schedule 9), it is clearly appropriate that CD could be acquired where all the relevant considerations are made out, including necessity and proportionality. This is because generally the acquisition of CD on a targeted basis is less intrusive than the powers for which the threshold under section 263(1) is relevant.

3.36 For all other serious offences, within the meaning of section 86(2A), care should be taken when applying for CD. In addition to the sentencing threshold and, separately, to the necessity and proportionality considerations relevant public authorities should also consider a number of factors when deciding the seriousness of a crime. These include, but are not limited to:

- the particular circumstances of the case;
- the offender;
- impact on the victim;
- the harm suffered; and
- the motive for the crime.

Trade Unions

3.37 As set out in the Act, the fact that the information that would be obtained under an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the authorisation is necessary on the grounds on which authorisations may be given. Public authorities are permitted, for example, to apply for an authorisation against members or officials of a trade union where that is necessary for one of the statutory purposes so long as the authorisation is proportionate to what is sought to be achieved.

4 Roles

Overview

This chapter outlines the key roles involved in the acquisition and oversight of CD.

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

- the applicant;
- the CD Single Point of Contact ('CD SPoC');
- the senior responsible officer ('SRO') in a public authority;
- the authorising individual.

The applicant

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

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

The Communications Data Single Point of Contact ('CD SPoC')

4.4 The CD SPoC is an individual trained to facilitate the lawful acquisition of CD and effective co-operation between a public authority, the Investigatory Powers Commissioner's Office ("IPCO") (formally Office for Communications Data Authorisations/"OCDA") and, where relevant, TOs and POs. To become accredited an individual must complete a course of training appropriate for the role of a CD SPoC and have been issued the relevant CD SPoC unique identifier. The Home Office will work with public authorities to ensure appropriate training is available for CD SPoCs, including by, where appropriate, authorising authorities to carry out training, maintaining a list of such authorities and monitoring and evaluating the training. Where this work is relevant to law enforcement, the Home Office will work with the College of Policing and a CD Professional Oversight Board as appropriate. The Home Office provides authentication services to enable TOs and POs to validate CD SPoC credentials.

4.5 Public authorities are expected to provide CD SPoC coverage for all CD acquisitions that they reasonably expect to make. (E.g., as police forces would expect to deal with a threat to life situation at any time, they must ensure that a CD SPoC is always available).

4.6 A CD SPoC promotes efficiency and good practice in ensuring only practical and lawful applications for CD are made. This encourages the public authority to regulate itself. The CD SPoC provides objective judgement and advice to the public authority on the application. In this way the CD SPoC provides a "guardian and gatekeeper" function helping to ensure that public authorities act in an informed and lawful manner. If a public authority is unable to call upon the services of an accredited CD SPoC, they should not seek to undertake the acquisition of CD.

4.7 The increase of communications media (including mobile telephony, internet communications and social media) and the ability for one individual to use multiple forms of communications means that the knowledge and experience of a CD SPoC is vital to advise and guide an applicant to make appropriate applications and acquire the data necessary for an investigation.

4.8 Public authorities may have multiple SPoCs working together. A SPoC from one organisation may assist another organisation where there is a joint investigation.

4.9 For each individual application, the roles of the applicant and CD SPoC will usually be carried out by two different people depending on how the organisation allocates it's CD SPoCs. In exceptional cases, both roles may be carried out by the same person. This may be appropriate for specific and specialist units who handle sensitive work and who have decided to combine the applicant/CD SPoC role to ensure better application of the principles of this Code. An organisation is also permitted to allow one individual to carry out the role of the applicant for one application and then as a CD SPoC for another application. Within all contexts, individuals acting as CD SPoC must be accredited and all CD applications must clearly detail who is acting and in what capacity (see paragraph 4.4 and 5.4).

The Senior Responsible Officer ('SRO')

4.10 Within every relevant public authority, there should be a SRO who must be of a senior rank within the authority - this must be at least the same rank as the DSO specified in Schedule 4. Where no DSO is specified the rank of the SRO must be agreed with the Home Office. The SRO is responsible for:

- the integrity of the process in place within the public authority to acquire CD;
- engagement with authorising individuals in IPCO (where relevant);
- compliance with Part 3 of the Act and with this Code, including responsibility for novel or contentious cases and with ensuring that errors are recorded, reported and managed appropriately (see paragraph 8.45);
- oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- ensuring the overall quality of applications by the public authority, with a particular focus on ensuring the continued proportionality of CD applications in long-running investigations and approving the submission of applications concerning Misconduct in a Public Office and the acquisition of cell site data relevant to devices in a specified area. This applies in respect of CD applications under section 60A submitted to IPCO.
- engagement with the IPC's inspectors when they conduct their inspections;
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPC; and
- ensuring compliance with any error reduction procedures that have been set out/agreed with the Home Office/IPC.

The authorising individual

4.11 CD applications can be authorised by three separate categories of individual depending on the circumstances of the specific case. References in this Code to 'authorising individual' refer to:

- An **authorising individual in IPCO**: section 60A of the Act confers power on the IPC to authorise certain applications for CD. In practice the IPC will delegate these functions to his staff.

- The **designated senior officer ('DSO')**: a person holding a prescribed office or rank in a relevant public authority is responsible for authorising certain applications where the requirement for independent authorisation does not apply.
- A **Judicial Commissioner**: a person who holds or has held judicial office, appointed under section 227 of the Act, who is responsible for approving requests to identify or confirm journalistic sources.

4.12 Individuals who undertake the role of authorising individual should have working knowledge of human rights legislation and this Code.

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

Operational independence of the designated senior officer

4.14 A DSO granting authorisations under section 61 of the Act related to operations or investigations must be independent from those operations or investigations (section 63(1)). In practice this means that a DSO should be far enough removed from the applicant's line management chain or the investigation to not be influenced by operational imperatives (e.g., pressure to expedite results on a particular operation). Usually this will mean that the DSO is not within the same department/unit or an integral part of the investigation. It is not considered good practice for applicants to be able to choose a DSO on a case-by-case basis, though this will sometimes be required if an assigned DSO is, for example, absent or unwell. Section 63 does not apply to urgent applications made under section 61A.

4.15 In exceptional circumstances a public authority may not be able to call upon the services of a DSO who is independent from the investigation or operation[4]. This may include cases where there is an immediate threat to life or another emergency (section 63(2) of the Act).

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

- where the investigation or operation concerned is one where there is an exceptional need, in the interests of national security, to keep knowledge of it to a minimum; or
- where there is an opportunity to obtain information where the opportunity is rare, the time to act is short, and the need to obtain the information is significant and in the interests of national security.

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

4.18 Where a DSO is not independent from the investigation or operation, they must explicitly record their involvement, and their justification for undertaking the role of the DSO.

[4] See section 63 of the Act.

5 Application process

Overview

5.1 The Act provides for acquisition of CD by way of an IPA Part 3 authorisation, an IPA Part 6 bulk acquisition warrant or other lawful authority.

5.2 This chapter sets out the application process that will apply when applying for an IPA Part 3 authorisation and involves:

- the making of an application (paragraphs 5.3 to 5.5);
- consultation with a CD SPoC (paragraphs 5.23 to 5.33); and
- authorisation by an authorising individual (paragraphs 5.34 to 5.45).

Making an application

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

5.4 An application to acquire CD must:

- describe the CD required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- describe whether the CD relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation and, where known, include their name. Where the name of the subject of the request is unknown, an alias may be used. Where the name of the subject of the request is known an alias can only be used in exceptional circumstances;
- include the operation name (if applicable) to which the application relates;
- identify and explain the time scale within which the data is required, more details on this can be found at Annex D;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it. (See section on necessity and proportionality, beginning at paragraph 3.3. This also applies to the next two bullets on collateral intrusion and unintended consequences);
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application and how these might be mitigated;
- where data is being sought from a TO or PO, specify whether the TO or PO may inform the subject(s) of the fact that an application has been made for their data; and
- where data is being sought in relation to offences where the serious crime threshold applies, there is additionally the need to consider the matters listed

at paragraph 3.34 to confirm that the particular case in question and the particular circumstances do justify CD being obtained.

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

Count Queries

5.6 An understanding of the number of unique entities likely to be returned by a request for data may, in some circumstances, provide useful context to an application. For example, ICR Condition D allows an applicant to undertake subject detection by permitting ICR data to be disclosed based upon access to specified service(s) at specified time(s). An understanding of how many entities may be identified from such an application may assist an authorising officer in their deliberations concerning the proportionality of the request.

5.7 A “Count Query” asks the TO to determine how many unique entities would be returned if the relevant query were run on their network.

5.8 The result is a number representing how many unique entities would be returned. No other information is disclosed by the TO and therefore no CD is released.

5.9 As no CD is sought or disclosed in a standard “Count Query” a Part 3 authorisation is not required by the applicant. Public authorities should, however, maintain a record of such requests, allowing SPoC managers to provide oversight regarding the feasibility, legality and appropriateness of the request and to facilitate IPCO inspection.

5.10 Such queries are a helpful additional tool to ensure that relevant CD applications are proportionate.

5.11 Without knowing this information, the authorising officer’s role to assess whether the application is proportionate to what is sought to be achieved could be harder.

5.12 A “Count Query” also has the practical effect of enabling an applicant to adjust search criteria, such as reduction in time period sought or of internet services queried, to bring the application within proportionate limits.

5.13 A complex “Count Query” which could result in the obtaining of CD or use sequential wildcards to reconstruct data in the retained CD store is prohibited by this Code unless a relevant IPA authorisation is obtained.

5.14 TOs are invited to support this “Count Query” procedure and the processing of data for this purpose will likely be considered lawful and necessary under Article 6(1)(e) UK General Data Protection Regulation (‘GDPR’) as being “necessary for the performance of a task carried out in the public interest ...”

5.15 TOs should consider this processing as necessary to minimise the amount of data disclosed and to protect the rights of their customers, working with a public authority to manage the intrusion prior to an application under the IPA. This will allow a public authority, and those authorising the request, to be assured any data disclosed is proportionate and necessary for the investigation and reduces the collateral intrusion as far as is reasonably practicable on other customers.

5.16 "Count Queries" may also support other applications for CD including those relevant to IPA authorisations for Compound Queries which may utilise filtering within the TOs.

5.17 Compound Queries are prohibited by this Code from being submitted under the "Count Query" process itself, but the "Count Query" process is intended to support applications for IPA authorisations which uses a Compound Query as part of the proposed authorised conduct.

Internet Connection Records which overlap Authorised periods

5.18 Internet traffic flows can persist for extended periods ranging up to several hours or days. The record of a traffic flow, made up of one or more flow parts, therefore could traverse an authorised period, either commencing before the authorised period and extending into it or commencing within an authorised period but continuing beyond it, or indeed both.

5.19 Such a situation could occur when a video is being watched from an online streaming service. The connection to the video streaming service may persist before, during and after the authorised period.

5.20 Due to the nature of IP connections the likelihood of this happening in an ICR disclosure request is perhaps greater than may previously have been the case for telephony CD.

5.21 In each case however the internet traffic flows will at least be extant *during* the authorised period.

5.22 TOs may disclose all ICRs that fall within the authorised period. Where an ICR overlaps with the authorised period the TO shall disclose these overlapping ICRs. This is on the basis that the overlapping ICRs are data which is inextricably linked to the authorised data and that disclosure results in negligible additional intrusion.

Process a CD SPoC will follow

5.23 Advice and consideration given by the CD SPoC in respect of any application may be recorded in the same document as the application and/or authorisation. The CD SPoC will, as appropriate:

- assess whether the specific CD required from a TO or PO is inextricably linked to other data. (In the event that the required data is inextricably linked to, or inseparable from, other events data, the authorising individual must take that into account in their consideration of necessity, proportionality, collateral intrusion and unintended consequences);
- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of TOs or POs;
- engage with applicants to develop and implement effective strategies to obtain CD in support of operations or investigations;
- advise on and manage the use of the request filter, specifically in relation to the progress of requests through the filter and compliance by the filter with the relevant authorisation (see Chapter 11);
- advise on the interpretation of the Act, particularly whether a Part 3 authorisation is appropriate;

- provide assurance that Part 3 authorisations are lawful under the Act and free from errors;
- consider and, where appropriate, provide advice on possible unintended consequences of the application and ways to mitigate these;
- consider, where possible any cost and resource implications to both the public authority and the TO or PO of CD requirements.

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

5.25 Any conduct to determine the TO or PO that holds, or may hold, specific CD is not conduct to which the provisions of Part 3 apply. This includes, for example, establishing from information available to the public or, where necessary, from a service provider which provider makes available a specific service (e.g., a telephone number or an IP address).

5.26 Given the training undertaken by a CD SPoC and the on-going nature of a CD SPoC's engagement with TOs or POs, it is good practice to engage the CD SPoC to liaise with the TO or PO where a public authority seeks to acquire reference data.

Exceptional circumstances where you do not need to use a CD SPoC

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

5.28 Police forces and law enforcement agencies should never obtain CD without consulting a CD SPoC and should use CD SPoCs from partner forces or agencies where necessary through a collaboration agreement (see paragraphs 8.57-8.60).

5.29 This provision does not absolve a public authority of the requirement to provide adequate CD SPoC cover for their investigative needs. The provision recognises that there may be some circumstances where, despite the best efforts of the public authority concerned, a CD SPoC is suddenly unavailable (e.g., due to ill health). It is important that in such rare circumstances authorisations for CD can be managed in certain limited situations.

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

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

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

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

Authorisation of applications

5.34 Section 60A of the Act provides for the independent authorisation of CD requests by the IPC. IPCO Authorisations performs this function on behalf of the IPC. An authorising individual in IPCO Authorisations can authorise any request, for any purpose, from any public authority.

5.35 Section 61 provides for the authorisation of CD requests by DSOs. Where an application for CD is for the purpose of national security under section 61(7)(a), or economic well-being where relevant to national security under section 61(7)(c), an application may alternatively be authorised internally by a DSO in a public authority. The DSO must, except where provided for in the Act, be independent of the operation concerned (see paragraph 4.14).

5.36 A DSO may also authorise a request for CD where there is an urgent need to acquire the data because of an imminent threat to life or another emergency (see paragraphs 5.28 to 5.40 for further details).

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

5.38 The authorising individual is responsible for considering and deciding applications for CD. It is their responsibility to consider the application and record their decision at the time, in writing or electronically to show that they have understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny. In addition, the authorising individual may wish to make some written comments on the necessity and proportionality of the application. Written comments are not required in all cases but there are certain situations where they are mandated by this code. For example, if an authorising individual is not independent of the operation or if a SPoC is not available, or if the urgent process has been used If comments are made, they should be tailored to a specific application as this best demonstrates the application has been properly considered.

5.39 If the authorising individual believes the acquisition of CD meets the requirements set out in the Act and is necessary and proportionate in the specific circumstances, an authorisation will be granted. If the authorising individual does not consider the criteria for obtaining the data have been met the application should be rejected and/or referred back to the CD SPoC and the applicant.

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

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

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

5.43 Particular care should be taken by authorising individuals when considering any application to obtain CD to identify apparatus (such as a mobile telephone) at or within a location or locations and at or between times on a given date or dates where the identity of the apparatus is unknown (the regional representative of the National Police Chiefs Council will be in a position to offer additional advice to CD SPoCs where investigations or operations in their public authority are considering the acquisition of such data). Unless the application is based on information that the apparatus was present or was likely to have been present in a particular location or locations at a particular time or times it will, in practice, be rare that any conduct to obtain CD will be proportionate or the collateral intrusion justified.

5.44 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 TOs and POs will undertake to adapt their systems beyond the requirements of their normal business practice to be able to assist the relevant public authority in preserving life. The use of such bespoke systems must be proportionate, and any collateral intrusion justified, to the specific circumstances of any investigation or operation.

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

Urgent granting of an authorisation

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

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

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

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

- an immediate threat of loss or serious harm to human life - this may include those situations where, for example, there is serious concern for the welfare of a vulnerable person including children at imminent risk of being abused or otherwise harmed;
- an urgent operational requirement where, within no more than 48 hours of the urgent authorisation being granted, the acquisition of CD will directly assist the prevention or detection of the commission of a serious crime or the making of arrests or the seizure of illicit material, or where that operational opportunity will be lost;

- 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;
- a situation where there has been a loss of life or serious harm to an individual, or where a person is otherwise unable to identify themselves, and the acquisition of CD will assist with locating the next of kin of the affected individual where there are no other methods to locate the next of kin.

5.50 Where the purpose of an application is to identify or confirm the identity or role of an individual as a source of journalistic information, then the only circumstances in which an urgent authorisation may be appropriate is where there is an imminent threat to life. See Chapter 8 for further details.

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

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

5.53 Particular care must be given to the use of the verbal urgent process. When verbal authorisation is given, the CD SPoC, when relaying service of the verbal authorisation to the TO or PO, must make a note of the time, provide a unique reference number for the notice and the name (or identifier) and contact details of the CD SPoC and, if required by the TO or PO, their unique identifier. Where telephone numbers (or other identifiers) are being relayed, the relevant number should be read twice and repeated back by the TO or PO to confirm the correct details have been taken.

5.54 Written notice must be given to the TO or PO retrospectively within one working day of the verbal authorisation being given. Working day' means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday in any part of the UK – see section 263(1) of the Act. Failure to do so will constitute an error which may be reported to the IPC by the TO or PO and must be recorded by the public authority (see the section on errors in Chapter 15 'Keeping of records' for more details).

5.55 After the period of urgency (in some instances where life is at risk, for example in kidnap investigations, the period of urgency may be extended, for example, over a bank holiday weekend but the written record must be produced at the earliest practical opportunity), a separate written process should be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the CD SPoC will collate details or copies of control room or other operational logs which provide contemporaneous records of the consideration given to the acquisition of data, decision(s) made by the authorising individual and the actions taken in respect of the decision(s).

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

5.57 An urgent authorisation made under section 61A ceases to have effect after three days beginning with the date on which the authorisation is granted. For example, an authorisation granted on a Monday cease to have effect at 23.59 on Wednesday. Where an urgent authorisation is granted in relation to subscriber data requests, historical data, or in relation to cases that can be resolved within those three days

(such as missing persons), further IPCO authorisation is not required provided the CD is not needed on an ongoing basis.

5.58 Where an urgent application has been granted internally, and a public authority wishes to continue to acquire CD for more than three days, (e.g., to acquire events data on a forward-looking basis for 30 days), then a new request should be made under section 60A before the three days expires. An application should be submitted to IPCO Authorisations following the application process detailed in this Code. It is possible to make a new section 61A application where it is necessary. IPCO will inspect S61A applications therefore organisations must be prepared to justify multiple applications for CD to IPCO.

Refusal to grant an authorisation

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

5.60 Where a request is refused by an authorising individual in IPCO Authorisations, the public authority has three options:

- not proceed with the request;
- resubmit the application with a revised justification and/or a revised course of conduct to acquire CD;
- resubmit the application with the same justification and same course of conduct seeking a review of the decision by IPCO Authorisations. A public authority may only resubmit an application on the same grounds to IPCO Authorisations where the SRO, or a person of equivalent grade in the public authority, has agreed to this course of action. IPCO Authorisations will provide guidance on its process for reviewing such decisions.

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

6 Authorisations

Overview

This chapter sets out guidance and examples for public authorities who seek to use an authorisation of conduct to acquire CD or to give notice to obtain CD from a telecommunication operator or PO. It lays out the responsibility and expectations of the SRO, the CD SPoC and telecommunication operator or PO in relation to authorisations.

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

- conduct to acquire CD which may include the public authority obtaining CD themselves or asking any person believed to be in possession of, or capable of obtaining, the CD to obtain and disclose it; and/or,
- the giving of a notice allowing the public authority to require by a notice a TO to obtain and disclose the required data.

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

- there is an agreement in place between a public authority and a TO or PO to facilitate the secure and swift disclosure of CD. Many TOs and POs have auditable acquisition systems in place to ensure accurate and timely acquisition of CD, while maintaining security and an audit trail;
- where the data can be acquired directly from a telecommunication system and the activity does not constitute interception or equipment interference; or
- a public authority considers there is a requirement to identify a person to whom a service is provided but the specific TO or PO has yet to be conclusively determined as the holder of the CD.

6.3 An authorisation to give a notice may be appropriate where a TO or PO is known to be capable of disclosing (and, where necessary, obtaining) the CD (for further detail see paragraphs 6.21- 6.31).

6.4 Where a TO or PO has provided a system to facilitate the secure and swift disclosure of CD, the fact that a request is received from an authenticated CD SPoC acting for a relevant public authority, or from a secure system of a relevant public authority or of the Secretary of State, shall be taken as adequate assurance that a lawful authorisation exists when the following additional information is provided:

- the unique reference number (‘URN’) of the authorisation;
- the date when the authorisation was granted;
- a description of the CD to be disclosed and, where relevant, the period of time the authorisation is intended to cover; and
- where appropriate, an indication of any time periods within which the data needs to be obtained.

6.5 An authorisation of conduct to acquire CD must:

- specify or describe (section 263(1) explains that “specified” in relation to an authorisation or notice means “specified or described” in the authorisation or notice. Therefore, “specify” is to be read accordingly as meaning either “specify”

or "describe") the conduct which is authorised and describe the CD to be acquired by that conduct specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the conduct is authorised, by reference to a statutory purpose under of the Act;
- include a unique reference number;
- specify the identity, rank or position (or unique identifier) of the authorising individual granting the authorisation.
- where applicable, confirm in writing that a CD SPoC has been consulted on this application;
- record the date and, when appropriate to do so, the time when the authorisation was granted;
- specify when the CD is to be obtained and disclosed by use of the request filter;
- if engaging the request filter, specify whether the processing of data (and its temporary retention for that purpose) is authorised and, if so, provide a description of the data that may be processed and the type or nature of processing to be performed (e.g. geographic correlation, IP address resolution);
- if engaging the request filter or acquiring ICRs, specify whether any threshold for the number of results returned is set which would prevent any portion of records being disclosed; and
- where data is being sought from a TO or PO, specify whether the TO or PO may inform the subject(s) of the fact that an application has been made for their data.

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

- specify or describe the operator[5] to whom the notice applies and the nature of requirements to be imposed;
- confirm whether a TO or PO may disclose the existence of this requirement, or any related pursuant authorisation or notice, to a customer or other individual.

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

6.8 The original or a copy of the authorisation must be retained by the public authority and be accessible to the CD SPoC.

6.9 When drafting authorisations within the meaning of sections 60A and 61 of the Act, the authorising individual must ensure, where possible, the description of the required data corresponds with the way in which the TO or PO processes, retains and retrieves its data for lawful disclosure. TOs and POs cannot necessarily or reasonably edit or adapt their systems to take account of every possible variation of what may be specified in authorisations, particularly via CD acquisition systems.

6.10 Some TOs or POs permit the lawful acquisition of CD by CD SPoCs via secure auditable CD acquisition systems. Where a CD SPoC has been authorised to obtain data from such a system, but concludes that the data cannot be acquired directly, the CD SPoC may provide the TO or PO with details of the authorisation in order to seek disclosure of the required data.

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

[5] The telecommunications operator or postal operator should be specified (named) wherever reasonably practicable.

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

- a victim reports receiving nuisance or threatening telephone calls or messages;
- a person who is the subject of an investigation or operation is identified from intelligence to be using a specific communication service;
- a person who is the subject of an investigation or operation is identified during an investigation (such as a kidnap) or from detailed analysis of data available to the public authority to be using a specific communication service;
- a mobile telephone is lawfully seized, and CD is to be acquired relating to either or both the device or its SIM card(s); or
- a witness presents certain facts and there is a need to corroborate or research the veracity of those, such as to confirm the time of an incident they have witnessed.

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

6.14 At the time of granting an authorisation of conduct to acquire CD or to give a notice in order to obtain specific CD, an authorising individual may also authorise, to the extent necessary and proportionate at that time, the acquisition of specific entity data relating to the CD to be obtained. This is relevant where there is a necessary and proportionate requirement to identify with whom a person has been in communication, for example:

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

6.15 At the time of granting an authorisation of conduct to acquire CD or to give a notice in order to obtain specific CD, an authorising individual may also authorise, to the extent necessary and proportionate at that time, the acquisition of other events data. This is relevant where there is a necessary and proportionate requirement to identify a person from the CD to be acquired, and the means to do so requires the TO or another TO to query their events data information, for example:

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

6.16 Where there is a requirement to acquire follow on entity or events data, following the acquisition of the specific data prescribed in an application, this proposed additional acquisition of data must be described in that application in such manner as to allow the authorising individual to be able to appreciate its foreseeability (see paragraph 6.18) and the level of intrusion that will occur as result of this additional data and be able to make a decision judging its necessity and proportionality. The

application does not need to prescribe the specific data that will be acquired as it may not be possible to do so prior to the acquisition of the primary data. Once the core operational objective of the application (e.g., to identify the user or an identifier or to locate the user of a service) has been achieved, no further requests for data can be made under that authorisation.

6.17 Examples include:

- An application for IP login history (events data) can be made to include subsequent requests for IP subscriber checks (entity data) on the identified IP addresses at specific dates and times, as well as further subscriber checks (entity data) on any telephone numbers retrieved through those IP subscriber records. This course of TO products will support the common objective of identifying the individual(s) using a particular online identifier. The CD SPoC can describe in the application that they will seek these additional data checks and how this will support the applicant's objective and the Authorising Individual can understand this course of action and provide an informed authorisation decision on this basis.
- Staged applications will be appropriate where the CD SPoC intends to first acquire a subscriber or customer record in relation to a known telephone number of interest, and only if that subscriber record does not assist the investigation, (e.g. it comes back as a pre-paid number with no further details) would the CD SPoC then additionally acquire call data (events data) over a specified period in order to assist with the identification of the individual, perhaps by comparing to known intelligence. Call data may still be required, regardless of the result of the entity check, if further evidence of attribution is required to support the investigation.
- An application is made to identify the user of a social media account and includes data to request IP login history for any email addresses identified as a result of the social media account information. This could also be treated as a staged approach where IP logins would initially be requested for a shorter period of e.g. two weeks before requesting IP logins for a longer period of e.g. three months only if no actionable data is retrieved from the shorter period of data.

6.18 It is the duty of the SRO in a public authority to ensure that the public authority makes available to the CD SPoC and the authorising individual such information as the SRO thinks necessary to ensure the integrity of any requirements for the acquisition of entity data to be obtained directly upon the acquisition or disclosure of any events data, and their compliance with Part 3 and with this Code. Ordinarily the applicant or other person within the investigation or operation will prepare a schedule of data, for example telephone numbers, to enable the CD SPoC to undertake the acquisition of subscriber information. The schedule will include details of the person who prepared it, cross reference it to the relevant notice or authorisation and specify the events data from which the data are derived.

6.19 The CD SPoC would normally be the person who takes receipt of any CD acquired from a TO or PO and would normally be responsible for its dissemination to the applicant. CD SPoCs in public authorities should be security cleared in accordance with their own organisation's requirements. When handling, processing, and distributing such information, CD SPoCs must comply with local security policies and operating procedures. CD acquired by public authorities must also be stored and handled in accordance with duties under relevant data protection legislation, see Chapter 12 for further details of data protection safeguards.

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

Notices in pursuance of an authorisation

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

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

6.23 Once the authorising individual has authorised the giving of a notice, it will be given to a TO or PO in writing or, in an urgent situation, communicated to the TO or PO orally. 'In writing' can include, but is not limited to, letter, fax, email, or via a secure portal operated by the TO or PO.

6.24 The notice should contain enough information to allow the TO or PO to comply with the requirements of the notice.

6.25 A notice must:

- describe the CD to be obtained or disclosed under the notice specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the requirements being imposed and the TO or PO on whom the requirements are being imposed;
- specify the manner in which the data should be disclosed and specify or describe the person(s) to whom the data is to be, or may be, disclosed or how to identify such person(s);
- include a unique reference number (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) and identify the public authority (where a relevant public authority is in a collaboration agreement, only the public authority to which the officer giving the notice belongs need be identified in some way);
- specify the name (or unique identifier), the office, rank and the position of the officer creating or giving the notice (A CD SPoC unit operating a triage-based operation can have two different CD SPoCs within the notice process. In a scenario that CD SPoC A had requested to give notice, CD SPoC B can submit the notice on behalf of CD SPoC A to the TO);
- be given in writing or, if not, in a manner that produces a record, within the public authority, of its having been given;
- record the date when the giving of a notice was authorised by the authorising individual;
- where appropriate, provide an indication of any urgency or time within which the TO or PO is requested to comply with the requirements of the notice;
- include an explanation that compliance with the notice is a requirement of the Act unless the notice is cancelled. A TO or PO which has not complied before the period of validity for the authorisation expires is still required to comply. The notice should contain sufficient information including the contact details of the CD SPoC to enable a TO or PO to, where necessary, confirm the notice is authentic and lawful; and

- if permission has been given, confirm the TO or PO may disclose the existence of this requirement, or any related pursuant authorisation or notice, to a customer or other individual.

6.26 The original or a copy of the notice must be retained by the public authority and be accessible to the CD SPoC.

6.27 A TO or PO is not required to do anything under a notice which it is not reasonably practicable for it to do, see section 66(3) of the Act.

6.28 A notice may only require a TO or PO to disclose the CD to the public authority. This will normally be to the public authority's CD SPoC.

6.29 Ordinarily the TO or PO should disclose, in writing or electronically, the CD to which a notice relates within agreed service levels or, where there are no agreed service levels, not later than the end of the period of ten working days from the date the notice is served upon the TO or PO. Defined service levels may be endorsed by the Secretary of State following agreement between the TO or PO, public authorities and IPCO, for example where a retention notice includes requirements to provide for data to be transmitted efficiently and effectively in response to requests.

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

6.31 Section 85 of the Act provides that where a notice under Part 3 is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given in any of the following ways:

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

7 Duration, renewals and cancellations

Overview

This chapter sets out the duration and renewal process of authorisations and notices. Authorisations should fulfil the consideration of necessity and proportionality and be for the shortest period of time.

Duration of authorisations and notice

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

7.2 Authorisations granted internally under section 61A in relation to urgent cases are valid for three days (see paragraph 5.57).

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

7.4 All authorisations should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s) e.g., details of events data on a specific date or for a specific period or the details of a subscriber on a specific date or for a specific period. Any period should be clearly indicated in the authorisation. The start date and end date should be given, and where a precise start and end time are relevant these must be specified. In the case of IP address, any timings must include an explicit indication of which time zone applies to those timings. Where the data to be acquired or disclosed is specified as ‘current’, the relevant date should be taken to be the date on which the authorisation was granted by the authorising individual. There can be circumstances when the relevant date or period cannot be specified other than ‘the last transaction’ or ‘the most recent use of the service’.

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

7.6 Authorising individuals should specify the shortest possible period of time for any authorisation. To do otherwise would impact on the proportionality of the authorisation and impose an unnecessary burden upon the relevant TO(s) or PO(s).

Renewal of authorisations

7.7 Any valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation. Authorisations will cease at 23.59 on the last day, with any subsequent renewal commencing at 00.00 hours the following day.

7.8 An authorisation cannot be renewed if it has already expired. If an application for renewal is reviewed by the authorising individual when the initial authorisation or

renewal has expired, the application for renewal will need to be rejected. Therefore, applicants should ensure that they send through an application for renewal ahead of the expiry of the former authorisation, taking into consideration the expected period of time it will take the authorising individual to review the application.

7.9 Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasons for seeking renewal should be set out by an applicant in an addendum to the application upon which the authorisation being renewed was granted. A renewal is not required if the request for CD was notified to the TO before the expiry of the CD authorisation, but the TO has not responded before the CD authorisation expires.

7.10 A renewal will not be granted if the conduct requested is expanding, instead, this should form the content of a new application. The reasons for seeking renewal should include explanation of what has been done to date, what CD has been received, how that CD assists with the investigation and whether the objectives have been met in full or are still progressing. This is not required with a staged approach to an investigation, for example where consequential enquiries have been approved after an initial application for CD.

7.11 Where an authorising individual is granting a further authorisation to renew an earlier authorisation, this can include an authorisation that has been renewed previously, they should:

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

Cancellation of authorisations

7.12 A DSO who has granted an authorisation under section 61 or 61A of the Act must cancel it if, at any time after the granting of the authorisation[6], it is no longer necessary for a statutory purpose, or the conduct required by the authorisation is no longer proportionate to what was sought to be achieved. An authorisation may otherwise be cancelled at any time by the DSO.

7.13 Where an authorisation has been granted by an authorising individual under section 60A it may be cancelled at any time by the public authority or IPCO Authorisations, and must be cancelled if, at any time after the granting of the authorisation, it is no longer necessary for a statutory purpose, or the conduct required by the authorisation is no longer proportionate to what was sought to be achieved.

7.14 In practice, it is likely to be the public authority that is first aware that the authorisation is no longer necessary or proportionate. In such cases the CD SPoC (having been contacted by the applicant, where appropriate) must cease the authorised conduct.

7.15 A notice given under an authorisation (and any requirement imposed by a notice) is cancelled if the authorisation is cancelled but is not affected by the authorisation ceasing to have effect at the end of one month period of validity. Reporting the cancellation of a notice to a TO or PO should usually be undertaken by the CD SPoC in a public authority at the earliest opportunity. If the authorisation being cancelled relates to an urgent operational situation that has been resolved, or has

[6] This can include a renewed authorisation.

changed, it may be appropriate for the senior officer dealing with the situation, on the ground or in a control room, to notify the TO or PO (or arrange for their notification) that the notice imposed under an authorisation is cancelled where that person has the earliest opportunity to do so.

7.16 The cancellation of an authorisation to give a notice where the notice has been reported to a TO or PO must:

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

7.17 In cases where the CD SPoC has initiated the cancellation of an authorisation given under s61 or s61A for serving a notice and has reported the cancellation to the TO or PO, a DSO (or another officer filling that role) should confirm the decision for the CD SPoC either in writing or, if not, in a manner that produces a record of the notice having been cancelled by a DSO. Where the DSO who authorised the giving of the notice to the TO or PO is no longer available, this duty should fall on a person who has temporarily or permanently taken over the role.

7.18 In cases where the CD SPoC has initiated the cancellation of an authorisation given under section 60A for serving a notice and has reported the cancellation to the TO or PO, neither IPCO Authorisations nor a DSO need to confirm the cancellation. All authorisations granted by IPCO Authorisations can be cancelled without referring back to IPCO Authorisations.

7.19 Cancellation of an authorisation should:

- identify, by reference to its unique reference number, the authorisation being withdrawn;
- record the date and, when appropriate to do so, the time when the authorisation was cancelled; and
- for section 61 and section 61A authorisations, record the name and the office, rank or position held by the DSO (or officer filling that role) authorising cancellation.

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

8 Further restrictions and requirements in relation to applications

Overview

This chapter sets out guidance on collaboration agreements and provides direction for public authorities who seek to acquire CD which relates to certain professionals or is novel and contentious in nature. The chapter includes examples of when it is necessary to receive judicial commissioner approval prior to submitting requests for CD.

Local authority procedures

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

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

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

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

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

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

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

Communications data involving certain professions

8.8 The fact a communication took place does not disclose what was discussed, considered or advised within the communication. However, the degree of interference with an individual's rights and freedoms may be higher where the CD being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (medical doctors, lawyers, journalists, parliamentarians, or ministers of religion).

8.9 It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with members of the above groups. This does not prevent an application for CD being made about or in connection to the above groups/professions. In a situation where an application for CD is required applicants must draw attention to any circumstances that may lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and freedom of expression within their consideration of necessity and proportionality (see paragraphs 3.3 to 3.31). For the same reason, the authorising individual must take care when authorising these applications and consider whether there might be unintended consequences of the application and whether the public interest is best served by the application.

8.10 Section 2 of the Act makes clear that public authorities and IPCO Authorisations must have regard to whether the level of protection to be applied in relation to any acquisition of CD is higher because of the particular sensitivity of that information. For example:

- the identity of a journalist's source, or
- communications between a parliamentarian and their constituent.

This is a non-exhaustive list of examples. Applicants should consider a wide range of persons who may hold sensitive information within this context.

8.11 Applicants must make it clear and record within applications that the CD requested is of individuals known to be in sensitive groups/professions outlined in paragraph 8.8. The application must include the profession and these applications should be marked for the IPC's attention at the next inspection. Refer to Chapter 15 for more details.

Applications for communications data relating to journalists and their sources

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

8.13 It is in the UK public's interest, and in accordance with Article 10 of the European Convention of Human Rights that the free press and freedom of expression is protected as part of a democratic society, which includes the willingness of sources to provide information to journalists anonymously. Where the intention is to request data in order to identify a source of journalistic information, the public interest justifying the request must override the public interest in protecting the source.

8.14 A source of journalistic information is an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be

so used. Throughout this Code any reference to 'sources' should be understood to include any person acting as an intermediary between a journalist and a source.

8.15 An assessment of whether someone is a journalist (for the purposes of the Act) should be made on all the facts and circumstances available at the time of the application. Consideration should be given to:

- the frequency of an individual's relevant activities;
- the level of professional rigour they seek to apply to their work;
- the type of information that they collect;
- how they disseminate that information; and
- whether they receive payment or renumeration for their work.

8.16 This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech and reflect the role that journalists play in protecting the public interest.

8.17 Where a public authority is unclear as to whether an individual may be considered to be a journalist, they should seek advice before authorising a relevant application (see paragraph 8.23).

8.18 Applications for CD in relation to journalists and their sources may still be made but public authorities and authorising individuals will want to take particular care in preparing and authorising such applications. To ensure that an application made to acquire CD relating to a journalist or source is lawful it is crucial that public authorities and authorising individuals correctly apply the process set out in this chapter.

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

8.20 Where the purpose of an application is to identify or confirm the identity or role of an individual as a source of journalistic information, Judicial Commissioner approval must be sought prior to the acquisition of the CD taking place, other than where there is an imminent threat to life. Where an application relates to journalists but is not intended to identify or confirm the identity or role of an individual as a source of journalistic information, judicial approval is not required but care should be taken.

8.21 CD alone may not be sufficient to identify a source, consequential action and other information is likely to be required. Identifying communications addresses does not in itself provide sufficient information to determine the nature of a relationship. However, where such authorisations are given with the intention that the information obtained will be used as part of an assessment of the identity of a source, this will require Judicial Commissioner approval.

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

8.23 Where appropriate, public authorities should seek advice on the overarching application of these provisions from their own legal team first, then the Home Office, and then IPCO. In addition, where an application may be considered novel or contentious, authorising individuals should follow the processes set out at paragraph 8.48 onwards.

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

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

8.25 Where an authorising individual has granted an authorisation for this purpose in circumstances other than in relation to an immediate threat to life (see below) the authorisation will not take effect until such time as a Judicial Commissioner has authorised it under section 77 of the Act.

8.26 Public authorities that are required to have applications for CD, sought for any of the purposes in 60A(7), authorised by IPCO Authorisations by virtue of section 60A of the Act should take account of the considerations set out in this section before submitting the application to IPCO Authorisations. IPCO Authorisations will consider the request for CD, and where this request is authorised, they will seek the approval of the decision by a Judicial Commissioners before responding to the public authority except where there is an imminent threat to life (see paragraph 8.34 for further detail).

8.27 Public authorities authorising CD applications internally by virtue of sections 61 or 61A of the Act must submit an application to a Judicial Commissioner for approval after it has been authorised by a DSO except where there is an imminent threat to life. An application under section 61A may be made in cases where there is emergency other than a threat to life.

8.28 In addition to applications specifically intended to identify a journalist's source, the acquisition of CD to confirm existing understanding or corroborate other evidence of the identity of, or role of an individual as a journalist's source requires approval by a Judicial Commissioner.

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

8.30 Public authorities should give careful consideration before seeking to acquire CD to identify or confirm who within a public authority may have leaked information to the media. Such an application should only be made pursuant to a statutory purpose under Part 3 and where it is considered that there is a public interest in making such an application which overrides the public interest in source protection. Judicial Commissioner approval is required in such cases.

8.31 In addition to the requirements detailed in Part 3, an application to acquire CD for the purpose of identifying or confirming the role of an individual as a source should give special consideration to necessity and proportionality and specifically draw attention to the following matters:

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

- **Public interest in source protection**: consideration of whether the intrusion is justified, giving proper consideration to whether the public interest is best served by the application. The application should consider properly whether the suspected conduct is of a sufficiently serious nature for rights to freedom of expression to be interfered with. For example, authorising individuals need to apply special care in the case of applications concerning alleged 'whistleblowers' as special protections are afforded to such individuals in some legislation.
- **Collateral intrusion**: as well as consideration of the rights of the individual under investigation, consideration should also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. Any potential for unintended consequences of such applications should be considered.

8.32 It will not be sufficient to simply state that the matters have been appropriately considered. Further detail is required on how the matters apply in the case and any mitigations put in place.

8.33 Each public authority should keep a central record of all occasions when such an application has been made, including a record of the considerations undertaken (see Chapter 15 for more details). At the next inspection, such applications should be specifically marked for IPCO's attention.

Threat to life exception

8.34 In very limited circumstances an authorisation made for the purpose of identifying or confirming the identity or role of an individual as a journalist's source will not require Judicial Commissioner approval. If there is believed to be an immediate threat to life, such that a person's life might be endangered by the delay inherent in the process of obtaining Judicial Commissioner approval, the authorisation may take effect without such approval.

8.35 Examples of situations in which Judicial Commissioner approval may not be required due to an immediate threat to life include:

- a warning of an imminent terrorist incident being telephoned to a journalist or newspaper office;
- a journalist conducting an investigation which includes a significant element of personal danger who has not checked in with his office at the agreed time; or
- a source contacting a journalist to reveal their intention to commit suicide.

8.36 Such applications must be notified to the IPC as soon as reasonably practicable, as agreed with the IPC.

8.37 If additional CD is later sought for the purpose of identifying or confirming the identity or the role of an individual as a journalist's source as part of the same investigation, but where a threat to life no longer exists, Judicial Commissioner approval should be sought in the normal way.

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

8.38 The requirement for Judicial Commissioner approval does not apply where applications are made for the CD of those known or suspected to be journalists or sources but where the application is not to identify or confirm the role of an individual as a source of journalistic information. However, the application may still be sensitive and all those involved in it should proceed with care.

8.39 The following bullet points provide examples of when an application, which relates to a journalist or their source, may be considered not to be for the purpose of identifying or confirming the role of the individual as a journalist's source and as a result Judicial Commissioner approval may not be required.

- Where the journalist is a victim of crime and it is clear that their profession and sources are not relevant to the investigation.
- Where an identified source or suspected source is a victim of crime
- Where a journalist, identified source, or suspected source is a witness or other by-stander in an investigation not related to their roles as journalist or source and a CD application is made to discount them from the investigation.
- Where the journalist, identified source, or suspected source is suspected of committing a crime. (E.g., where a journalist is suspected of committing a crime and it is clear their profession and sources are not relevant to the investigation).
- To acquire the CD of a known criminal under investigation who is also a source.
- Where a journalist-source relationship is already confirmed
- Where an individual on a witness protection programme is concerned that an unsolicited caller is a journalist, or other individual, hoping to sell a story about the individual's new identity.

8.40 In each case authorising individuals should apply their own assessment to the specific circumstances of the case and identify whether there is any potential additional infringement of rights or intrusion to be considered, including whether the application should be considered novel or contentious (see paragraph 8.45). As this is a sensitive and often complex issue and the protection of Article 10 rights is crucial, it is important that authorising individuals proceed with caution and seek additional advice if there is any doubt as to whether Judicial Commissioner approval is required.

8.41 Where an investigation is conducted to prove criminal conspiracy between a journalist and their source, and the journalist-source relationship is already confirmed, Judicial Commissioner approval may not be required in all circumstances. For example, where specific facts about the timing or location of communications between the two individuals must be confirmed to prove the criminal conspiracy, Judicial Commissioner approval may not be required. An application for CD relating to a known or suspected journalist or a known or suspected source, which is not to identify or confirm the identity or role of an individual as a journalist's source, may still have an unusual degree of sensitivity attached to it. Where this is the case, the application should be considered potentially contentious and referred to the Judicial Commissioner for advice.

8.42 Legal Advice should be sought where applications are considered to fall into this category and then should be referred to the Judicial Commissioner. This includes, but is not limited to, applications for CD of a journalist or their source which are not to identify or confirm the identity or role of an individual as a journalistic source but:

- will likely result in the incidental and unintended identification or confirmation of a source (collateral intrusion into journalist sources); or
- relate to an investigation involving whistle-blowing or the leaking of documents or information to the media. For example, an application for the purpose of limiting reputational damage would not meet a statutory purpose and so would not be considered lawful.

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

- subscriber checks are authorised for all communications addresses in contact with a journalist over a period of time because, for instance, they are a victim of a serious crime;
- those checks are not for the purpose of identifying or confirming a source; and,
- information is already known about a source run by that journalist which will unavoidably result in the identification of that source if subscriber checks are obtained.

8.44 Particular care should therefore be taken to ensure that the application considers whether the intrusion is justified, giving proper consideration to the public interest. As well as consideration of the rights of the individual under investigation, consideration should also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. The officer needs to consider whether alternative evidence exists, or whether there are alternative means for obtaining the information being sought. Any potential for unintended consequences of such applications should be considered.

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

Judicial Commissioner Approval Overview

Situation / CD Application Aim[7]	Judicial Commissioner Approval Needed Prior to Requesting CD?
To identify/confirm the identity/role of an individual as a source of journalistic information.	Yes, unless threat to life situation.
Public authority seeks to authorise CD applications under sections 61 or 61A of the Act.	If identifying a journalistic source, yes (unless imminent threat to life).
To identify a journalist's source, to confirm existing understanding or corroborate other evidence of the identity of, or role of an individual as a journalist's source.	Yes, unless threat to life situation
To identify/confirm any identifying characteristic of a source, not solely their name. (E.g., home location or occupation).	Yes, unless threat to life situation.
Public authority suspects individual within that authority has leaked information to the media & requests CD.	Yes, carefully consider paragraph 8.30.
To identify/confirm the identity/role of an individual as a journalist's source as part of the same investigation & threat to life no longer exists.	Yes.
Journalist is a victim of crime & their profession/sources are not relevant to the investigation.	No
An identified source/suspected source is a victim of crime & their role as a source is not relevant to the investigation.	No
Journalist/identified source/suspected source is a witness/by-stander in an investigation not related to their role as journalist/source & aim is to discount them from the investigation.	No
Journalist/identified source/suspected source is suspected of committing crime & their profession/sources are not relevant to the investigation.	No
To obtain CD of a known criminal under investigation who is also a source.	No
Journalist-source relationship is already confirmed & the individual's role as a source is not relevant to the investigation.	No
Individual on a witness protection programme is concerned that an unsolicited caller is a journalist, or other individual, hoping to sell a story about the individual's new identity.	No
Application for those known/suspected to be journalists/sources but aim is not to identify/confirm the role of an individual as a source of journalistic information.	No
Relates to journalists but is not intended to identify/confirm the identity/role of an individual as a source of journalistic information.	No
Warning an imminent terrorist incident being telephoned to a journalist or newspaper office.	No, but notify the IPC as soon as possible.
Journalist's investigation includes someone who has not checked into his office at an agreed time & personal danger is present.	No, but notify the IPC as soon as possible.
Source contacted a journalist to reveal their intention to commit suicide.	No, but notify the IPC as soon as possible.

[7] This is a list of non-exhaustive examples, careful consideration should be applied to each investigation to ensure that CD applications are necessary and proportionate.

Novel or contentious acquisition

8.46 In recognition of the capacity of modern CD to produce insights of a highly personal nature, public authorities must take particular care where it is considered that a CD application, under Part 3, is novel or contentious. However, it is important to recognise that what might be considered novel or contentious by one public authority might be more routine for another. The following non-exhaustive list of examples might, depending on the specific circumstances, be considered novel or contentious:

- new technical methods of acquisition;
- new types of CD;
- applications which might result in an unusual amount of collateral intrusion but still be considered proportionate; and
- where there might be unusual sensitivity attached to the application regarding the nature of the target.

8.47 The fact that such applications could be novel or contentious does not preclude them being made, but it is important that the proper consideration set out below is given.

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

8.49 Where the public authority intends to require a TO or PO to undertake an action which of itself is novel or contentious, (e.g., a new technical method of data acquisition), the CD SPoC should consult the operator concerned.

8.50 A public authority may seek the advice of IPCO or a Judicial Commissioner before considering whether to embark on a course of action to acquire CD that could be considered novel or contentious. A public authority may also want to consider seeking legal advice first if appropriate. Such advice may be sought in relation to a single application or to an issue of principle that may be relevant to a number of future applications.

8.51 If sought, the public authority must record the views of IPCO. It is the responsibility of the SRO to maintain this record and a public authority should check against this information before seeking advice. This advice may be shared between public authorities to inform consideration of future applications.

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

8.53 Where a DSO is considering a request for CD that they consider to be novel or contentious they may seek advice from IPCO before authorising the application. Where the DSO proceeds against a recommendation from IPCO Authorisations or a Judicial Commissioner, the reasons for doing so must be recorded and these cases flagged to the Commissioner at their next inspection.

8.54 Where the DSO has doubt as to whether an application they have been asked to authorise is novel or contentious, they should consider seeking guidance from IPCO before deciding how to proceed.

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

8.56 Consideration should also be given to use of the Count Query provisions set out from paragraph 5.6 which allow the number of potential entities that may be returned by a novel or contentious application to be ascertained before an application is made. This may enable an applicant to more accurately and appropriately address questions of proportionality and collateral intrusion.

Public authority collaboration agreements

8.57 Any public authority may participate in a collaboration agreement, by which a CD SPoC and/or DSO of the supplying authority is put at the disposal of the subscribing authority. A public authority may be directed to enter into such an agreement by the Secretary of State. All local authorities must make applications through a CD SPoC at NAFN (see paragraph 8.1).

8.58 Public authorities must notify the Home Office of any plan to enter into a collaboration agreement. Before entering into an agreement, all parties to the agreement should consider:

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

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

- the issues identified in paragraph 8.57;
- the number and nature of applications made by a public authority; and
- the nature and function of the public authority concerned.

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

9 Considerations in relation to the acquisition of internet data

Overview

This chapter outlines the restrictions on which authorities can request ICRs. For those who are permitted to request ICRs, it is important to carefully consider the level of intrusion and assess the risk of collateral intrusion to ensure that ICR requests are necessary and proportionate. The chapter includes an explanation of Condition D, brought into the IPA via the IP(A)A 2024, and provides instructions on the use of Internet Protocol Address Resolution.

Internet Connection Records ('ICRs')

9.1 Under certain circumstances, an authorising individual may grant an authorisation to obtain data which requires the processing or disclosure of an internet connection record ('ICR') (see paragraph 2.91 for the definition of an ICR). Subject to paragraph 2.49 any application that involves the disclosure of ICRs must be authorised as events data.

9.2 All existing requirements regarding necessity and proportionality for authorisations to obtain CD also apply to the acquisition of ICRs. Authorising individuals should additionally have particular regard to the level of intrusion likely to result from disclosure of the data sought.

9.3 Section 62 of the Act recognises the additional sensitivities associated with ICRs. Local authorities may not acquire ICRs and public authorities can only require the disclosure or processing of ICRs under Part 3 for the purpose of identifying:

- the user of an internet service (either the person or apparatus);
- the internet communications services a device or person is using, (e.g., messaging applications) - an internet communication service is a service which provides for the communication between one or more persons over the internet and may include email services, instant messaging services, internet telephony services, social networking and web forums-;
- the internet services a device or person is using which wholly or mainly involve making available or acquiring material, whose possession is a crime (e.g., child abuse imagery) - an internet service is a service provided over the internet. It includes internet communication services, websites and applications-; or
- other internet services a device or person is using (e.g., to book travel).

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

9.5 The Act applies important restrictions when the statutory purpose for which ICRs are acquired is "the applicable crime purpose". In these circumstances ICRs can only be acquired for the prevention and detection of serious crime, as defined in s86(2A) of the Act, Condition D applications attract further restrictions (see paragraph 9.6 and 9.18).

9.6 The serious crime threshold does not apply to entity data applications made for the investigative purpose of identifying the sender of an online communication under Condition A (section 62(3)). Such applications will not result in the disclosure of a list of internet connection records as the service used will already be known. For example, a TO could be asked who was using a specified service at a known date/time. The data disclosed will take the form of related entity data only, (see identifying the sender of an online communication in paragraph 9.19 onwards). Should a request for this investigative purpose require the disclosure of any events data then the serious crime threshold will apply.

9.7 Where ICR events data is sought applications may be made by the public authority for the purpose of identifying:

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

9.8 Limitations on public authorities' access to ICRs are outlined in paragraph 9.3. These ICR event applications will require a TO to disclose a list of ICRs covering a specific time period. The information provided may include ICRs not directly relevant to the investigation but which are inextricably linked to those that are. Given the scope for collateral intrusion, the authorising individual will therefore need to apply careful consideration to ensure this period is proportionate and no longer than necessary.

9.9 Occasions when a public authority might seek ICRs to identify an internet communications service being used include, but are not limited to:

- to facilitate follow up with another communications provider in order to establish who a missing person was in contact with before their disappearance;
- where a device or individual is known to be communicating online but it is not known how; or
- to facilitate follow up with another communications provider in order to identify contacts of a suspect following the seizing of a communication device.

9.10 An ICR is unlikely to directly identify who a person has been communicating with online. The information that an ICR can provide is the service(s) that was used and the time that the service(s) was accessed, allowing further enquiries to be made of the relevant provider.

9.11 A public authority may seek ICRs to identify possible access to illegal information or to identify a subject's internet service use. Examples of scenarios include:

Aim: Establish access to illegal material	**Aim: Establish general internet service**

If a person suspected of posting or viewing illegal images has been accessing sites containing this information.	How and when a person, who is suspected of people trafficking, is communicating with victims, making travel arrangements, paying for goods and services associated with their activity and laundering their money.
If a person, suspected of owning or selling illegal weapons, has been accessing online marketplaces which wholly or mainly sell illegal items.	Identify any activity which may assist in locating a missing vulnerable person (e.g., identifying travel services or mapping applications).
If a person suspected of involvement in cybercrime has been accessing sites selling malware.	How and where an individual suspected of wholesale money laundering is hiding or dissipating illegal funds.

9.12 A public authority may only examine ICRs returned to them which do not directly relate to the purpose for which they were acquired (e.g., a record of access to a travel site returned in response to a request for communication services) where necessary and proportionate to do so for the purposes set out in sections 60A(7), 61(7) and 61A(7) of the Act. For further information see paragraphs 4.34 – 4.36 on excess data in the Notices Code of Practice.

9.13 Local authorities are prohibited from seeking the processing or disclosure of ICRs for any purpose, as outlined in paragraph 9.3.

9.14 There may be circumstances where it is more appropriate for public authorities to utilise alternative lawful powers available to them to obtain information which is similar to, or includes, ICR data (e.g., interception or equipment interference warrants). The use of alternative lawful powers will be subject to additional levels of authorisation. For example, a warrant must be issued by the Secretary of State (or Scottish Ministers as applicable) and approved by a Judicial Commissioner. Before using alternative lawful powers, the relevant authority must consider whether a less intrusive means of acquiring the data is appropriate.

Restrictions in relation to Condition D for Internet Connection Records

9.15 The Investigatory Powers (Amendment) Act 2024 inserted Condition D into section 62 of the Investigatory Powers Act in respect of ICRs for target detection purposes.

9.16 The IPA 2016 includes Condition A which requires certain thresholds to be met on the ‘known’ elements of an investigation, specifically unequivocal knowledge of which website or service has been accessed and in what period it has been accessed. The focus of Condition A is in identifying who was involved in an event that is known to have happened on the internet.

Example: Condition A

- Forensic analysis of a seized laptop identifies a specific event involving a video conferencing facility being used to live stream the abuse of a child on a known date and time.
- Condition A authorisation would be appropriate to identify the offender based on the known factors of 'service' and 'date/time of use'.

9.17 In contrast, Condition D allows for situations where a subject is assessed to be using one or more services in a given time period. Condition D removes the requirement to unequivocally *know* a specific time or times of access, and service in use, and instead allows these factors to be 'specified' within the application.

Example: Condition D

- Forensic analysis of a seized device identifies a website hosting illegal images of children and investigators wish to identify individuals who are accessing the website.
- Condition D authorisation would be appropriate as there is a reasonable belief that individuals are accessing the illegal content but the investigator will lack the necessary unequivocal knowledge for a Condition A authorisation.

9.18 Safeguards, restrictions and oversight are in place in respect of Condition D. Condition D:

- use is limited to only the intelligence services and the National Crime Agency ('NCA'). The intelligence services and NCA must ensure they have an understanding of the construct of the ICR data, appreciation of human versus machine generated connections, computer logic and the importance of accurate syntax. No other public authority is permitted to seek access to ICRs under Condition D.
- is limited to the "lawful purposes" relating solely to national security, the economic wellbeing of the UK (so far as those interests are also relevant to the interests of national security), and for the detection and prevention of serious crime. Serious crime is defined at section 86(2A) of the Act and, for the intelligence services, is further qualified by the meanings of serious crime in the Intelligence Services Act 1994 and the Security Service Act 1989.
- requires that, whilst absolute knowledge is not required, the service(s) and the period of time specified must be necessary and proportionate (see paragraphs 3.3 onwards). The applicant must explain their decision to use Condition D with reference to the supporting information and analysis where appropriate.
- requires that the applicant pay particular attention to the period of time sought ensuring that it is no longer than is absolutely necessary to meet the operational objective of the application. Whilst collateral intrusion is included within the assessment of proportionality, applicants must pay particular attention in addressing exactly how collateral intrusion will be managed to ensure that only those persons who should be the subject of further investigation are so. Applications under Condition D may be more subjective in nature. It is vital that the applicant addresses collateral intrusion where the services concerned are otherwise innocent in nature (as per the above legitimate video conferencing facility example at 9.16 for Condition A). This also applies when sites are illegal in nature as some access may concern

academic or journalistic research or otherwise be innocent/accidental in nature. Those authorising such applications must be satisfied that steps taken to address collateral intrusion will be sufficient to ensure that innocent parties are not impacted beyond what is necessary and proportionate.
- may necessitate that a number of internet services are layered together within an application along with relevant time periods. This can have the effect of increasing proportionality and limiting collateral intrusion by reducing the number of subjects of interest with each additional criteria specified in the application.

Identifying the sender of an online communication

9.19 Internet Protocol Address Resolution ('IPAR') is used to identify the sender of an online communication. IPAR is used when a public authority knows the 'source' IP address related to a communication of interest and needs to determine the customer linked to this address. There is often a pressing need for such requests (e.g., terrorism and child abuse investigations). Due to modern communications technology, this is often not a simple task and applications to acquire CD for this purpose must consider the associated complexities and balance these against the operational requirements.

9.20 To communicate on the internet a device must be allocated an IP address. A communication may be:

- between two users, in which case the IP address will normally relate to their personal electronic device or to the internet access point to which their device is connected;
- between two servers in which case the IP addresses will relate to the equipment in question; or,
- between a user's personal electronic device and a server, for instance a user downloading material from a website.

9.21 The implementation of network address translation and dynamic IP addressing means that an IP address may be shared amongst a number of customers simultaneously and sometimes for a short period of time (e.g., when allocated to a mobile device). In most cases, a communication over the internet will originate from the end-user's device and this will be the "source" IP address, and the communication will be received by the internet service, and this will be the "destination" IP address. The following paragraphs use source IP address and destination IP address in this way as this is the more common pattern. However, there are circumstances where the source IP address will be that of the internet service and the destination IP address will be that of the end-user's device. This does not change the fundamental meaning of this section. The following paragraphs will not make the technical distinction between the 'source' and 'destination' IP address but will refer to these only as the 'customer IP address'.

9.22 In order to enable the TO to identify a customer from their allocated IP address, the public authority must provide a minimum of one customer IP address and one date/time or range of time. To enable the identification of a person who initiated a communication, rather than the service used to send that communication, the public authority must provide a customer IP address which relates to a specific device operated by an individual not to a destination device such as a server.

9.23 However, where IP addresses are shared between network customers, providing just the customer IP address and the time of the communication will often not be sufficient for a TO to resolve the address to an individual customer. Public authorities should therefore ensure they include any other data that is available to

them with the application. For example, if there are more IP addresses and times (or time ranges) which they believe relate to the same device or person, then that data should also be provided to the TO. Other examples of data types include:

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

9.24 Where public authorities need to resolve IP addresses, ICR data will usually be the only additional data that is available. This is because they will already know the internet service that has been used by the device or person which they are trying to resolve. For example, if someone posts a bomb threat to an online blog, the blog's access records may provide the police with both the customer IP address allocated to the user who posted the threat and details about the server hosting the blog (such as the IP address of the server). In such circumstances, the police should provide both these IP addresses, plus any other information the blog records provide (such as port numbers used), to the TO as this will increase the likelihood that the TO will be able to accurately match these details to an individual customer. Paragraph 2.51 explains that the data requested rather than processed by the TO is the only issue relevant to the authorisation level.

9.25 Where a public authority provides a customer IP address to a TO to resolve it to a user, that request may require the TO to process ICRs. It will therefore be necessary to consider the restrictions in relation to ICRs.

9.26 Where the public authority is aware there is a possible risk of increased collateral intrusion because the TO may give multiple customers the same IP address (this applies in the context of "natted" IP addresses) then any available ICR data which might assist the TO in narrowing down an answer should be provided by the public authority to the TO where possible to assist with reducing that collateral intrusion.

9.27 The TO may disclose the ICR data back to the public authority when it discloses the user of the source IP address in question (see paragraph 2.52 for further details on where a TO may disclose data originally provided by the public authority).

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

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

- the applicant should consider what data is available to them and base their application on those elements of data which will enable the TO to make the most appropriate and proportionate return;
- the applicant should use as many relevant identifiers as are available to them in making their application, in order to ensure that the TO may make the most appropriate return. Where more than one IP address or more than one date / time is available, the public authority should consider resolving more than one to allow cross-correlation of data sets;

- the authorising individual should take account of advice provided by the CD SPoC as to an appropriate strategy for the acquisition of IPAR data in each case;
- the authorising individual should consider whether to specify that data should only be returned where it can be linked to one individual or whether larger data sets may be returned. The authorising individual may decide to accept returns of larger data sets only where the necessity and proportionality case is sufficiently strong and must detail their considerations of proportionality in the authorisation;
- if the CD SPoC considers that data may be returned that links to more than one individual, they must, through consultation with the TO, provide the authorising individual with guidance as to the amount of data that is likely to be disclosed; and
- the authorising individual should consider where returns of incomplete data could lead to false positives or false negatives for an operation, and how this might be mitigated through the use of corroborating evidence. As a greater number of communications services become available, it is no longer possible to obtain full visibility of an individual's communications. Whilst the data available might only identify one individual who meets the specified criteria, the provision of further data regarding other communications methods might identify further matches, thus rendering the initial result a 'false positive'. The likelihood of 'false negatives' where individuals are ruled out of a case because they did not appear in a particular data set should also be considered.

9.30 The considerations above will also apply to authorisations where the public authority does not have an IP address but wishes to determine the individual that carried out a certain action online. For example, if a public authority has received a report indicating that an unknown individual used a specific internet service to upload child abuse imagery at a particular time, and has access to children, the public authority could make a Condition A ICR request as described in the section above concerning ICRs. For UKIC and the NCA only, it may be appropriate to use Condition D for the acquisition of ICRs to determine all users of the service over the specified timeframe, though again in conjunction with any other additional information that can be provided to the telecommunications operator in order to assist with the selection of the relevant records.

9.31 The particular issues associated with the complexity of IP address resolution mean that it is subject of specific rules jointly set by National Police Chiefs' Council ('NPCC') and IPCO and for the adherence of law enforcement personnel who undertake that activity. These can be found at Annex E.

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

Overview

This chapter sets out guidance for situations when the disclosure of CD is necessary and proportionate in the public interest, such as disclosure to the emergency services following an emergency call.

Sudden deaths, serious injuries, vulnerable and missing persons

10.1 There are circumstances when the police undertake enquiries in relation to specific matters of public interest where the disclosure of CD may be necessary and proportionate. Sections 60A(7) and 61A(7) of the Act specify certain purposes for which the acquisition and disclosure of CD may be necessary. These purposes assist the police in carrying out their functions. For example:

- identifying any person who has died or who is unable to identify himself because of a physical or mental condition, other than as a result of crime (e.g., in the case of a natural disaster or an accident);
- obtaining information about the reason for a person's death or condition;
- locating and notifying next of kin following a sudden or unexpected death;
- locating and notifying next of kin of a seriously injured person;
- 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; and
- for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

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

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

Public Emergency Call and SMS Service (999/112 calls)

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

10.5 This Code is not intended to regulate the handling of an emergency call but to ensure the boundary between this Code and the Public Emergency Communications Services Code of Practice is clear. In so doing this Code recognises an emergency period of one hour after the termination of the emergency call in which disclosure of CD to emergency services will not require a Part 3 authorisation. Such disclosure is a type of "lawful authority" for the purposes of section 11 of the Act.

10.6 The Act recognises this 'golden hour' provision following changes made as a result of the Investigatory Powers (Amendment) Act 2024. This amendment introduced a non-exhaustive list of authorities where a relevant person has lawful authority to obtain CD from a TO or PO. This includes circumstances where the CD is obtained by the relevant person for the purpose of enabling, or facilitating, the making of a response to a call made to the emergency services.

10.7 The Communications Act 2003 provides Ofcom with the power to set conditions that TOs must comply with in relation to emergency calls. TOs must ensure that any service user can access the emergency authorities by using the emergency numbers and, to the extent technically feasible, make caller location information available to the emergency authorities for all 999/112 calls. In practice this means sufficient detail to identify the origin of the emergency call and, if appropriate, to enable the deployment of an emergency service to the scene of an emergency. Whilst TOs and the emergency operator will seek to assist in identifying the location of the incident being reported, it remains the responsibility of the emergency services control room staff to obtain adequate address information from the caller to locate the incident.

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

10.9 TOs should take steps to assure themselves of the accuracy of the information they may be called upon to disclose. Any known limitations in this accuracy, particularly for location, should be proactively disclosed to the emergency services. Emergency services should be aware that CD may not always be available for disclosure by the TO depending on the particulars of the communications service used to make the call.

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

10.11 The emergency service can call upon an emergency operator or relevant service provider to disclose data about the maker of an emergency call within the emergency period one hour from the termination of the 999/112 call. Such circumstances will amount to lawful authority under the provisions set out in section 11.

10.12 It is appropriate for the emergency service or emergency operator to require the TO to disclose any further caller location information that might indicate the location of the caller at the time of the emergency call. Within one hour of the 999/112 call, it is also appropriate for the TO, acting in the belief that information might assist the emergency service to respond effectively or efficiently to the emergency, to proactively disclose to the emergency service or emergency operator any further information about the location of the caller at the time of the emergency call or a new location the caller has moved to, if it is within the one hour period.

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

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

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

10.16 If the emergency call is clearly a hoax, there is no emergency. Where an emergency service concludes that an emergency call is a hoax and the reason for acquiring data in relation to that call is to detect the crime of making a hoax call – and not to provide an emergency service – then an appropriate lawful route should be used to acquire the data.

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

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

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

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

Malicious and nuisance communications

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

10.22 Where the complainant reports a matter to the police that has been previously raised with the TO or PO, any data already collated by the TO or PO may be disclosed to the police CD SPoC in accordance with relevant data protection legislation. However subsequent police investigation that may require the

acquisition or disclosure of additional CD should be requested from an operator under the provisions of the Act.

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

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

11 The request filter

Overview

This chapter outlines guidance on request filters. It explains what a request filter is, how a public authority can use it, how the data will be managed, how long the data will be retained and how the oversight of a public authority's use of a request filter is conducted.

11.1 The request filter provides an additional safeguard in relation to the acquisition of CD. It works alongside other acquisition safeguards and existing infrastructure to limit the volume of CD being provided to a public authority.

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

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

- providing a mechanism for pulling fragmented CD together and providing a more complete analysis. With the increasing use of a wider range of online communications services and communications networks, the CD required to answer operational questions is becoming more fragmented;
- reducing analytic burden on public authorities and getting an operational answer in the shortest possible time to facilitate the timely recovery of evidence, discount individuals without further, more intrusive activity, and identify witnesses while events remain fresh in their memories; and
- managing proportionality and collateral intrusion. A public authority will only be provided with the data that directly answers its question, as opposed to all the data originally required to conduct the analysis.

Authorisations

11.4 The request filter can be used to obtain and process data as part of a CD authorisation.

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

11.6 The request filter may be identified as part of the approach to managing collateral intrusion in an authorisation. The request filter will only disclose records that match specified criteria to the CD SPoC and applicant. In making such a case, the authorisation should consider the likely effectiveness of the specified criteria in achieving the expected reduction in records. For example, a large number of people are likely to be in both Brighton Station at 07.30 on a Monday and London Victoria at 09.00 the following Thursday.

11.7 The authorising individual, with advice from the CD SPoC and taking account of information provided by the request filter on the volumes of data that may be disclosed, must consider the proportionality of:

- the data to be disclosed to the request filter by the TOs or POs; and
- the data to be disclosed to the applicant by the request filter.

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

11.9 The authorising individual must also consider the proportionality of the data to be disclosed to the request filter by the TOs or POs, even if the majority is not expected to be released to the public authority.

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

Making use of the request filter

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

11.12 The request is sent to the filter which in turn identifies the relevant TOs or POs for the request and requires them to disclose the authorised CD only to the request filter. They will not be aware of the detail of the processing to be undertaken.

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

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

Data management

11.15 The request filter will be operated on behalf of the Secretary of State by the Home Office.

11.16 The data controller for any authorised CD disclosed by a TO to the request filter will be the public authority. The data processor for all data disclosed to the request filter will be the Home Office (or another public authority designated by the Secretary of State by regulations). Once any data is disclosed to a public authority, that public authority continues to be the data controller for that disclosed data.

11.17 The CD associated with an authorisation will be temporarily retained in the request filter until either the authorised processing is complete or, it ceases to be necessary to retain the data for the purpose concerned, whichever is the sooner. Data that is no longer necessary will be deleted from the filter.

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

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

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

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

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

- providing authorising individuals with information to inform decisions on the necessity and proportionality of authorisations;
- support, maintenance, oversight, operation or administration of the arrangements; and
- the functions of the IPC.

11.23 This information may only be disclosed to:

- authorising individuals for the purposes of determining the necessity and proportionality of an authorisation;
- individuals designated by the Secretary of State for the purposes of support, maintenance, oversight, operation or administration of the request filter;
- the IPC for the purposes of the functions of the IPC; or
- when otherwise authorised by law.

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

- protection of personal data disclosed by TOs or POs to the request filter in accordance with an authorisation;
- controls, monitoring and audit of access to and use of the request filter;
- restrictions regarding disclosure of results from the request filter;
- provisions for deletion of material when no longer necessary or proportionate to retain it; and
- those provisions set out in Chapter 12 regarding data protection.

11.25 Data disclosed to the public authority as a result of use of the request filter must be handled in accordance with Chapter 12.

Oversight and reporting

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

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

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

11.29 The error reporting provisions detailed in Chapter 15 apply to the request filter. Should any significant processing errors occur which give rise to a contravention of any requirements in Part 3 of the Investigatory Powers Act, the fact must be reported to the IPC immediately. Where one technical system error occurs, it could have multiple consequences. Such errors could, for example include the omission of, or incorrect matches in filtered results, or the release of results that exceed specified thresholds. For more detail see Chapter 15.

12 General safeguards

Overview

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

12.1 CD acquired or obtained under the provisions of the Act may only be held for one or more of the statutory purposes for which the public authority can acquire CD. Such data as is held should be adequate, relevant and not excessive in relation to the purpose.

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

12.3 CD held by a public authority should be treated as information with a classification of OFFICIAL and a caveat of SENSITIVE, though it may be classified higher if appropriate. Details of government security classifications can be found at https://www.gov.uk/government/publications/government-security-classifications. Those who do not use these classifications should treat information in the appropriately equivalent manner under their data security rules. The SENSITIVE caveat is for OFFICIAL information that is subject to “need to know” controls so that only authorised personnel can have access to the material. This does not preclude, for example, the disclosure of material or the use of this material as evidence in open court when required. Rather, the classification and caveat of OFFICIAL - SENSITIVE makes clear that CD must be treated with care, noting the impact on the rights to privacy and, where appropriate, freedom of expression of the subjects of interest and, depending on the data, possibly some of their communications contacts.

12.4 CD that is obtained directly as a consequence of the execution of an interception warrant must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 53 of the Act.

12.5 CD acquired under the Act and all copies, extracts and summaries of it, must be held in a manner which provides an adequate level of protection for the relative sensitivity of the data and meets the data protection principles set out in the relevant data protection legislation. Data must be effectively protected against unauthorised access and use, with particular consideration given to the principles of data security and integrity.

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

12.7 A public authority may disclose CD acquired under the Act only to the minimum extent necessary. The individual or organisation to which it is to be disclosed must require access for purposes compatible with those in the Act. On occasions where it is necessary for a public authority to disclose data to an overseas authority, the process outlined in paragraphs 12.29 – 12.31 should be followed.

12.8 When sharing data, the relevant public authority must be satisfied that the data will be adequately protected and that safeguards are in place to ensure this. Subject to the exceptions set out in paragraphs 12.29-12.31 (disclosure of CD to overseas

authorities) data shared must be afforded the same protections as it would receive at the public authority which originally acquired it. Appropriate limitations must be placed on the number of people to whom material is disclosed and the extent to which material is disclosed.

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

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

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

12.12 Where it is necessary to process CD acquired under the Act together with data from other sources, the public authority must ensure that either it remains possible to identify the source of the data and apply security provisions accordingly or that the resultant combined data is subject to the highest security standard applicable.

Disclosure of communications data and subject access rights

12.13 This section of the Code provides guidance on the relationship between disclosure of CD under the Act, TOs' or POs' obligations to comply with a notice to disclose data, and individuals' right of access under relevant data protection legislation to personal data held about them.

12.14 The offence at section 82 of the Act does not override the right, provided in the data protection legislation, for a person to request access to a copy of their personal data. However, the data protection legislation provides for the ability to exempt from specified obligations and rights in the legislation, including the right of access. As a result, where such a request is received, a TO or PO will want to consider whether any of the exemptions are applicable. Exemptions which may be applicable in this context include:

- The national security exemption, which enables exemption from specified provisions, including subject access rights, where it is required for the purposes of safeguarding national security[8].
- The "crime and taxation" exemption, which enables exemption from specified provisions, including subject access rights, to the extent that complying with those provisions would be likely to prejudice the prevention and detection of crime and the apprehension or prosecution of offenders[9].

[8] The exemption is provided for at section 28 of the DPA 2018. The ICO has published guidance on the applicability of the exemption – available online at National security and defence exemption: a guide | ICO

[9] This exemption is provided for in Para 2 of Schedule 2 to the DPA 2018. The ICO has published guidance on the applicability of the exemption – available online at A guide to the data protection exemptions | ICO.

12.15 The exemption from subject access rights does not automatically apply. In the event that a TO or PO receives a subject access request where the fact of a disclosure under the Act might itself be disclosed, the TO or PO concerned must carefully consider whether, in the particular case, disclosure of the fact of the authorisation engaged the need to rely on an exemption.

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

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

12.18 Where a TO or PO is uncertain whether disclosure of the fact of a notice would be likely to prejudice an investigation or operation, it should approach the CD SPoC of the public authority which gave the notice and do so in good time to respond to the subject access request. The CD SPoC must provide a response which will enable the TO or PO to comply with its obligations to respond to the subject access request within 40 days at the latest. The CD SPoC can make enquiries within the public authority to determine whether disclosure of the fact of the notice would likely be prejudicial to the matters set out in paragraph 10.19 of the Notices Codes of Practice. If the public authority does not want the fact of the notice to be disclosed to the subject, then they must provide the TO or PO with sufficient justification as to the exemptions.

12.19 Where a TO or PO is responding to a request from an individual and relies on an exemption provided in the data protection legislation to withhold a piece of information, 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.

12.20 TOs and POs should keep a record of the steps they have taken in determining whether disclosure of the fact of a notice would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police. Under data protection legislation, an individual may make a complaint to the Information Commissioner who can assess whether a subject access request has been handled in compliance with such legislation.

Acquisition of communication data on behalf of overseas authorities

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

12.22 There are two methods by which CD, whether obtained under the Act or not, can be acquired and disclosed to overseas public authorities - this includes public authorities within the Crown Dependencies and the British Overseas Territories:

- judicial co-operation; or

- non-judicial co-operation.

12.23 Neither method compels UK public authorities to disclose data to overseas authorities. Data can only be disclosed when a UK public authority is satisfied that all relevant conditions imposed by domestic legislation have been fulfilled.

Judicial co-operation

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

12.25 If such an MLA request is accepted by the central authority, it will be referred for consideration by the appropriate public authority in the UK. The application may then be considered and, if appropriate, the request used to produce a Part 3 CD application under the Act. This should then be submitted to the appropriate authorising individual in line with the guidance in this Code of Practice.

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

Non-judicial co-operation

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

12.28 The UK public authority must be satisfied that the application complies with UK obligations under human rights and data protection 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

12.29 Where a UK public authority is considering the acquisition of CD on behalf of an overseas authority and the transfer of the data to that authority, it must consider, as with any data transfer, whether the data will be adequately protected outside the UK and what safeguards may be needed to ensure that protection. Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

12.30 If the proposed transfer is to an authority outside of the UK Europe, then it may be disclosed if the overseas authority can ensure an adequate level of data protection.

12.31 The UK public authority must decide in each case whether the data will be adequately protected overseas before transferring any data. Data protection legislation recognises that it will not always be possible to ensure adequate data protection in countries outside of the UK. There are exemptions to the principle such

as where the transfer of data is necessary for reasons of ‘substantial public interest.’ There may be circumstances when it is necessary for CD to be disclosed to a third-party country even though that country does not have adequate safeguards in place to protect the data (e.g., in the interests of national security). That is a decision that can only be taken by the public authority holding the data on a case-by-case basis. Advice may be sought from the relevant Government department or the Information Commissioner’s Office where required.

13 Notification

Overview

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

Duty to consider notification

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

13.2 Where it would not be damaging to investigations, the public authority may allow the TO or PO to notify the individual, (e.g., when the TO or PO receives a subject access request under data protection legislation). Where it would be damaging to investigations the public authority, must make clear that the TO or PO is not permitted to notify the individual that their data has been acquired.

Notification of serious errors under the Act

13.3 As identified in Chapter 15 of this Code, there may be rare occasions when CD is wrongly acquired or disclosed. In these cases, the public authority which made the error, or established that the error had been made, must report the error to the authority's SRO and the IPC. In accordance with section 231 of the Act, when an error is reported to the IPC, the IPC may inform the affected individual, who may make a complaint to the IPT.

13.4 In considering whether to notify an individual of an error, the IPC must be satisfied that the error is:

- a serious error; and
- it is in the public interest for the individual concerned to be informed of the error (see paragraph 15.37 onwards).

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

Notification in criminal proceedings

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

13.7 Where CD is used to support the prosecution case it will be served as evidence on the defendant. Even where the CD is not being relied upon to support the prosecution case, in compliance with its disclosure obligations pursuant to the

Criminal Procedure and Investigations Act 1996 ('CPIA'), the prosecution will reveal the existence of CD (and potentially the material generated in the process of it being obtained) to a defendant on a schedule of non-sensitive unused material, if that data is relevant (data may be relevant if it has some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case). Such material will be provided to the defendant if, pursuant to section 3 of the CPIA, such material might reasonably be considered capable of undermining the prosecution case and/or assisting the defence case.

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

13.9 If, through any of the above notification processes, an individual suspects that their CD has been wrongly acquired, the IPT provides a right of redress. As set out further in paragraph 17.3, an individual may make a complaint to the IPT without the individual knowing, or having to demonstrate, that any investigatory powers have been used against them.

14 Compliance and offences

Overview

This chapter outlines the expectations of a TO or PO to fulfil the requirements asked of them via a Part 3 notice. It includes guidance on a technical capability notice, an acquisition offence and a disclosure offence.

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

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

14.3 Where 'technical capability notice' or 'data retention notice' obligations apply, an operator will be considered as having put in place the capabilities specified in that notice when consideration is given to whether the steps they are required to take under Part 3 of the Act are reasonably practicable.

14.4 When considering whether it is reasonably practicable for a person outside the UK to comply with a notice, section 85(4)(a) specifies that regard must be had to any requirements or restrictions under the law of the country where the TO or PO is based that are relevant to the taking of those steps. It also makes clear the expectation that TOs and POs will seek to find ways to comply without giving rise to conflict of laws. What is reasonably practicable should be agreed after consultation between the TO or PO and the Government. If no agreement can be reached it will be for the Secretary of State to decide whether to proceed with civil proceedings.

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

Offences

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

Acquisition Offence

14.7 Under section 11 of the Act, it is an offence for a person in a public authority, knowingly or recklessly, to obtain CD from a private sector TO or PO without lawful authority.

14.8 The purpose of section 11 in the Act is to prevent public authorities from acquiring CD from TOs without a clear lawful authority. Under section 11 of the Act, it is an offence for a person in a public authority listed in Schedule 4 to the Act to knowingly or recklessly to obtain CD from a TO or PO without lawful authority. It is not meant to prevent public authorities from sharing CD with

another public authority where it is necessary and proportionate for them to do so. The section 11 acquisition offence therefore does not apply to public authorities which acquire CD from another public authority which is acting as a TO in relation to that CD.

14.9 The following are examples of cases where a relevant person in a public authority has lawful authority to obtain CD from a telecommunications operator or postal operator. This is a non-exhaustive list of authorities and includes the following:

- where the relevant person's obtaining of the CD is lawful for all purposes in accordance with section 81(1) of the Act; e.g. they have sought an IPA Part 3 authorisation);
- any other case where the relevant person obtains the CD in the exercise of a statutory power of the relevant public authority; e.g., in the context of a civil investigation or for regulatory or supervisory purposes (refer to section 12 schedule 2 abolition or restriction of general information gathering powers));
- where the operator lawfully provides the CD to the relevant person otherwise than pursuant to the exercise of a statutory power of the relevant public authority (whether or not in the exercise of a statutory power to disclose); e.g. the operator provides the CD to the public authority voluntarily;
- where the CD is obtained in accordance with a court order or other judicial authorisation;
- where the CD had been published before the relevant person obtained it, for example academic research; or,
- where the CD is obtained by the relevant person for the purpose of enabling, or facilitating, the making of a response to a call made to the emergency services; e.g., when a person has made a call to the police, fire, rescue and ambulance services and His Majesty's coast guard. This information is normally only available from the telecommunications operator for the period of 60 minutes following that call. After that a Part 3 authorisation will normally be required in relation to that CD.

14.10 Public authorities should be aware that situations may arise where there are a number of lawful authorities available to obtain CD. This Code cannot account for all eventualities, but in these situations public authorities must be aware of their legal obligations, act responsibly, take great care to ensure that they obtain CD in the most appropriate way.

14.11 Public authorities should be aware that conscious and deliberate decisions to lawfully obtain CD outside of an IPA Part 3 authorisation are likely to be closely scrutinised by the IPC. Public authorities should be prepared to justify any such decisions. The IPC must keep under review functions relating to the acquisition or retention of CD that are exercisable under the Act, so may need to investigate, for example, any acquisition of CD suspected of being deliberately designed to avoid appropriate safeguards.

14.12 Where CD could be acquired through a Part 3 IPA authorisation but a public authority judges that it is more appropriate to use another lawful authority, the IPC may, as part of their oversight of the regime, require further justification and evidence of the decision-making process if, for example, there is a suspicion that the acquisition of CD has been deliberately designed to avoid appropriate safeguards.

14.13 The creation of the offence of unlawfully obtaining CD reflects the sensitivity of CD and the need for careful consideration in authorisation of its acquisition. The roles and responsibilities laid down for the SRO, DSO and SPoC are designed to prevent

the knowing or reckless acquisition of communications by a public authority where it does not hold a lawful authorisation. Proper adherence to the requirements of the Act and this Code, including following the procedures identified in Chapter 4 will mitigate the risk of any offence being committed.

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

14.15 This offence is not designed to capture errors on behalf of the public authority but rather, for example, instances where a person in a public authority failed to take account of obvious risk or where a person in a public authority deliberately fails to obtain an authorisation or obtains CD from a TO or PO despite the fact that they could not have genuinely believed they have lawful authority .

14.16 In particular, it is not an offence for a public authority to obtain CD where it is made publicly or commercially available by the TO or PO or otherwise where the TO or PO freely consents to its disclosure. In such circumstances the consent of the operator provides the lawful authority for obtaining the data.

Disclosure Offence

14.17 Under section 82, it is an offence for a TO to disclose, without reasonable excuse, the existence of an authorisation or notice for CD under the Act.

14.18 The offence of unauthorised disclosure occurs when any TO or PO, or an employee of/a person working on behalf of a TO or PO, reveals the existence of a requirement to disclose CD about a particular person to that person or reveals the existence of any request following an authorisation to disclose such data (e.g., CD about a particular person to that person). The purpose of these provisions is to prevent the potential for informing criminal suspects or subjects of interest that their data has been sought and, consequently, prevent the risk of informing them that they are under suspicion.

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

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

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

- the interests of other public authorities in the operation or investigation;
- any potential negative impact on future operational or investigative capability; and
- the undermining of the purposes outlined in section 60A(7), 61(7) and 61A(7) of the Act.

14.22 Circumstances in which it may be appropriate to give permission to disclose the existence of a specific authorisation or notice for CD may include where CD is required to be disclosed to assist in the investigation of a crime of which the subject of the authorisation or notice is the victim (e.g., where a person's phone has been stolen and the police seek CD in order to locate the phone). However, this will always depend on the specific circumstances of the investigation.

14.23 It is very unlikely to be a reasonable excuse for a TO or PO to disclose such information in the interests of transparency to its customers without the permission of the relevant public authority.

Section 3

General matters

15 Keeping of records

Overview

This chapter outlines the responsibility and expectations of a public authority, TO and PO to record and retain information. It includes guidance on the handling and processing of relevant and reportable errors, serious errors and excess data.

Records to be kept by a relevant public authority

15.1 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 should be held centrally by the CD SPoC or in accordance with arrangements previously agreed with the IPC.

15.2 These records must be available for inspection by the IPC and retained to allow the IPT, established under Part 4 of Regulation of Investigatory Powers Act 2000 ('RIPA'), to carry out its functions. The IPT will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates, particularly where continuing conduct is alleged. Although records are only required to be retained for at least three years, it is desirable, if possible, to retain records for up to five years.

15.3 This Code does not affect any other statutory obligations placed on public authorities to keep records under any other enactment - for example the relevant test given in the Criminal Procedure and Investigations Act 1996 and the code of practice under that Act, which requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor.

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

(i) the number of applications submitted by an applicant to a CD SPoC seeking the acquisition of CD (including orally);

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

(iii) the number of applications submitted to an authorising individual for a decision to obtain CD (including orally), which were approved after due consideration;

(iv) the number of applications submitted to an authorising individual for a decision to obtain CD (including orally), which were referred back to the applicant or rejected after due consideration, including the reason for doing so;

(v) the number of authorisations of conduct to acquire CD granted (not including urgent oral applications);

(vi) the number of authorisations to give a notice to acquire CD granted (not including urgent oral applications);

(vii) the number of notices given pursuant to an authorisation requiring disclosure of CD (not including urgent oral applications);

(viii) the number of times an urgent application is approved orally;

(ix) the number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of CD;

(x) the priority grading of the authorisation for CD including urgent oral authorisations;

(xi) whether any data that is requested is that of a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, member of a relevant legislature, or minister of religion) (and if so, which profession) - see paragraphs 8.8 – 8.45 on CD involving certain professions for more information -;

(xii) the number of times an authorisation is granted to obtain CD in order to confirm or identify a journalist's source; and

(xiii) the number of items of CD sought, for authorisation granted (including orally) . One item of CD is a single communications address or other descriptor included in a notice or authorisation. For example, one communications address that relates to 30 days of incoming and outgoing call data is one item of CD.

15.5 These records should distinguish between requests considered by IPCO Authorisations under section 60A and those considered by DSOs under sections 61 and 61A, where it is possible to do so (e.g., only for 15.4.ii to 15.4.xiii, where the statutory power has been selected).

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

(i) the unique reference number (URN) allocated to the application, authorisation and where relevant the notice;

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

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

(iv) whether the item of CD is events or entity, as described at section 261(5) of the Act, and Chapter 2 of this Code;

(v) a description of the type of each item of CD included in the notice or authorisation (the data type is to include whether the data is telephone data, whether fixed line or mobile, or internet data, or postal data. Guidance on specific data types to be collected may be issued by, or sought from the IPC);

(vi) whether the item of CD relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;

(vii) the age of the item of CD. Where the data includes more than one day, the recorded age of data should be the oldest date of the data sought;

(viii) where an item of data is event data retained by the TO or PO, an indication of the total number of days of data being sought by means of notice or authorisation (in the case of a forward-facing authorisation, the number of days of data sought will often differ from the number of days of data disclosed or acquired. A forward-facing authorisation could be withdrawn or cancelled at the point it has served its purpose. For example, if the purpose is to identify an anticipated communication between two suspects, the authorisation may be withdrawn subsequent to that communication being made); and

(ix) the TO or PO from whom the data is being acquired.

15.7 Where the advice of a Judicial Commissioner or IPCO Authorisations has been sought prior to the acquisition of CD that could be considered novel or contentious, the public authority must record the views of IPCO Authorisations or the Judicial Commissioner. It is the responsibility of the Senior Responsible Office to maintain this record.

15.8 A subset of these records must be sent in written or electronic form to the IPC, as specified and requested by them. Those records that are not requested by the IPC should continue to be retained by the public authorities as set out in paragraphs 15.1 to 15.7. Records from the public authority may also be requested by the Home Office to assess the use of CD and public authorities should share these records accordingly and in line with their own data sharing policy. Guidance on record keeping may be issued by the IPC. Guidance may also be sought by relevant public authorities or persons contracted by them to develop or maintain their information technology systems.

15.9 The IPC will not seek to publish statistical information where it appears to them that in doing so would be contrary to the public interest or would be prejudicial to national security.

Records to be kept by a telecommunications operator or postal operator (acquisition)

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

15.11 The records to be kept by a TO or PO, in respect of each authorisation must include:

- the identity of the public authority (this can be a code or an abbreviation);
- the Unique Reference Number ('URN') of the authorisation;
- the date the relevant details of the authorisation were disclosed to the TO or PO; and
- the date when the CD was disclosed to the public authority or, where secure systems are provided by the TO or PO, the date when the acquisition and disclosure of CD was undertaken.

15.12 TOs and POs must also keep sufficient records to be able to provide confirmation of the exact CD that has been disclosed in the event of later challenge in court. TOs and POs should retain this data or record for a period of up to two years. This may comprise the data that was disclosed, a copy of the response, or a digital record that could be used to validate the response but should contain no more data than is necessary to verify the authenticity of such disclosures in court - a digital signature is an electronic record of a disclosure and would assist the court in verification of the origin and integrity of the data throughout the acquisition, investigation and prosecution process. Where a digital signature is held there should be no need to retain the underlying data. In exceptional cases and with prior written agreement, TOs may retain the URN and cryptographic digest for an extended period.

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

Records to be kept by a telecommunications operator or postal operator (retention)

15.14 To assist the Information Commissioner to carry out their statutory function in relation to the Act, TOs and POs must maintain a record of information that indicates whether and how they have complied with the provisions of this Code. Such information must be provided to the Commissioner on request.

15.15 Such records may include but are not limited to:

- data retention & disclosure system access audit records;
- IT Health Check security reports;
- security incident logs;
- data retention volumes;
- details of retained financial records (i.e. Payment Card Industry Data Security Standard implications and required exemptions);
- data destruction records;
- hardware (storage media) destruction records; and
- documentary evidence to demonstrate how the TO or PO has fulfilled its responsibilities under Chapter 5 regarding security, integrity and destruction of retained data in the Notices Code of Practice.

15.16 Guidance on the maintenance of records by TOs and POs to assist with the Information Commissioner's statutory functions in relation to the Act may be issued by or sought from them.

Errors

15.17 This section provides information regarding errors. Proper application of the Investigatory Powers Act as amended by the Investigatory Powers (Amendment) Act 2024 and thorough procedures for operating its provisions, including for example the careful preparation and checking of applications, notices and authorisations, should reduce the scope for making errors whether by public authorities, TOs or POs.

15.18 Any failure by a public authority or such other persons providing assistance to apply correctly the process of acquiring or obtaining CD set out in this Code will increase the likelihood of an error occurring. Wherever possible, technical systems should incorporate functionality to minimise errors. A person holding a senior position within each public authority must undertake a regular review of errors and a written record be made of each review.

15.19 Section 231 of the Act makes specific reference to a "**relevant error**", which is defined in section 231(9) of the Act as an error:

- by a public authority complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner; and
- of a description identified for this purpose in a Code of Practice under schedule 7.

15.20 A CD "relevant error" occurs where both of the following conditions are met:

- there has been an error by a public authority in complying with any requirements imposed by the Act (or any other enactment) which are subject to review by the Investigatory Powers Commissioner; and
- the CD has been acquired or disclosed wrongly.

15.21 Errors can have significant consequences on an affected individual's rights and, in accordance with section 236(6) of the Act, all relevant errors must be reported to the Investigatory Powers Commissioner by the public authority that is aware of the error.

15.22 When a relevant error has occurred, the public authority which made the error, or established that the error had been made, must report the error to the authority's SRO and then notify the IPC as soon as practicably possible, and no later than five working days after it has been established by appropriate internal governance processes that a relevant error has occurred. Such internal governance processes are subject to review by the IPC. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

15.23 From the point at which the public authority identifies that a relevant error may have occurred, they must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so.

15.24 A full report must be sent to the IPC by the public authority as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it

has not been possible to provide the full report within five working days of establishing the fact of the error, the reasons this is the case. Where the report is being made by the public authority that made the error, that report should also include: the cause of the error; any unintended collateral intrusion; any analysis or action taken; and a summary of the steps taken to prevent recurrence.

15.25 As set out at section 231 of the Act, the IPC will keep under review the definition of relevant errors. The IPC may also issue guidance as necessary, including guidance on the format of error reports. The intelligence services must have regard to any guidance on errors issued by the IPC.

15.26 Where any error occurs in the granting of an authorisation, the giving of a notice or as a consequence of any authorised conduct – including use of the request filter, or any conduct undertaken to comply with a notice, a record should be kept.

15.27 A relevant error must be reported to the IPC by whoever is responsible for it. For example, where the error has occurred because the relevant public authority provided incorrect information, the public authority must report the error.

15.28 Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of CD that require further improvement to eliminate errors and the risk of undue interference with any individual's rights. Such errors can have significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, result in the individual being wrongly detained or wrongly accused of a crime as a result of that error.

15.29 This section of the Code cannot provide an exhaustive list of possible causes of relevant or reportable errors. Examples could include:

Relevant errors:

- an authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under the Act;
- human error, such as incorrect transposition of information from an application to an authorisation or notice where CD is acquired or disclosed;
- acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation; and
- the omission of, or incorrect matches in filtered results, or the release of results that exceed specified thresholds.

Reportable errors:

- a notice has been given which is impossible for a TO or PO to comply with;
- 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[10];

[10] 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.

- failure to serve written notice (or where appropriate an authorisation) upon a TO or PO within one working day of urgent oral notice being given or an urgent oral authorisation granted;
- where an error has occurred but is identified by the public authority or the TO or PO without data being acquired or disclosed wrongly; and
- human error, such as incorrect transposition of information from an application to an authorisation or notice where CD is not acquired or disclosed.

Error made by TO or PO

15.30 It is the responsibility of the TO to notify any potentially affected public authority of a reportable error, as soon as reasonably practicable from the time they identify the error and provide the public authority with data to enable them to undertake investigations to assess and rectify any impact this may have. This should include the public authority's reference(s) and the associated identifier, such as MSISDN, relevant to the error.

15.31 Where a public authority reports to the IPC the mistake made by a TO or PO, the report must include details of the error and indicate whether the TO or PO has been informed or not (in which case the public authority must explain why the TO or PO has not been informed of the report).

15.32 Where material which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it is disclosed in error by a TO or PO, that material and any copy of it (including copies contained in or as attachments in electronic mail) should be destroyed as soon as the report to the IPC has been made.

Error made by the public authority

15.33 Where a TO or PO discloses CD, as a result of an error by the public authority, the TO or PO must report each such instance to the IPC within no more than five working days of the error being discovered.

15.34 A person holding a suitably senior position within a TO or PO should report the public authority's relevant error, identifying the error by reference to the public authority's unique reference number and providing details of any remedial action taken including steps taken, or to be taken, to prevent recurrence. Reportable errors by the TO's or PO could include responding to a notice by disclosing incorrect data or by disclosing the required data to the wrong public authority.

15.35 The records kept by a public authority accounting for relevant 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 SRO should undertake a regular review of the recording of such errors.

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

Serious errors

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

15.38 In deciding whether it is in the public interest for the person concerned to be informed of the serious error, the IPC must in particular consider:

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

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

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

Excess Data

15.41 Where authorised conduct by a public authority result in the acquisition of excess data, or its disclosure by a TO or PO to comply with the requirement of a notice, the excess data acquired or disclosed should only be retained by the public authority where appropriate to do so (e.g., in relation to a criminal investigation).

15.42 Where a public authority is bound by the Criminal Procedure and Investigations Act 1996 and its Code of Practice, there will be a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid authorisation. If a criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

15.43 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 SRO (or a person of equivalent grade in the public authority) will then consider the reason(s) and review all

the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. As with all CD acquired, the requirements of relevant data protection legislation must also be adhered to in relation to any excess data.

TO reporting of errors and personal data breaches

15.44 TOs and POs are required to report relevant errors made in response to authorisations or notices for CD under Part 3 to the IPC. TOs are also required to notify any Personal Data Breaches[11] that occur in relation to authorisations or notices under Part 3 of the Act to the Information Commissioner[12]. In some cases, a relevant error may also be a Personal Data Breach and so must be reported to both the IPC and the Information Commissioner ('IC'). A TO should consult with the public authority that the authorisation or notice relates to before reporting the error to the IPC or notifying the Information Commissioner's Office of the Personal Data Breach, to ensure consistent reporting or notification.

15.45 The Memorandum of Understanding between the IC and the IPC establishes how the IPC and the IC work together and share information, including in relation to Personal Data Breaches that also constitute relevant errors and are notified to the IC and reported to the IPC.

15.46 Where TOs are required to report personal data breaches that relate to conduct taken pursuant to, or in purported pursuance to, a Part 3 CD authorisation or notice to the ICO and the IPC, they also have obligations under s.235(2) IPA to ensure that, where the cause of the data breach may be ongoing, Judicial Commissioners have all the relevant information to inform the discharge of their functions, including their authorisation functions under s.60A of the Act.

[11] As defined in regulation 2(1) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI/2003/2426) (the 2003 Regulations).
[12] As required under regulation 5A(2) of the 2003 Regulations (subject to any relevant restrictions, as defined in section 235A of the Act, read with regulation 29(1)(a)(i) of the 2003 Regulations).

16 Oversight by the Investigatory Powers Commissioner and the Information Commissioner

The Investigatory Powers Commissioner

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

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

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

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

16.5 Anyone, including anyone working for a public authority, or a TO who has concerns about the way that investigatory powers are being used may report their concerns to the IPC. In particular, any person who exercises the powers described in the Act or this Code must, in accordance with the procedure set out in Chapter 15 of this Code, report to the IPC any relevant error of which it is aware. This may be in addition, or as an alternative, to the person raising concerns through the internal mechanisms within the public authority.

16.6 Should the IPC uncover, or be made aware of, what they consider to be a serious error relating to a person who has been subject to an investigatory power then, if it is in the public interest to do so, the IPC is under a duty to inform the person affected.

Further information on errors can be found in Chapter 15 of this Code. The public authority who has made the error will be able to make representations to the IPC before the IPC decides whether it is in the public interest for the person to be informed. Section 231(6) states that the IPC must also inform the affected person of any rights that the person may have to apply to the Investigatory Powers Tribunal.

16.7 The IPC must annually report on the findings of their audits, inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the public interest. Only the Prime Minister will be able to make redactions to the IPC's report.

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

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

The Information Commissioner

Please also refer to the Notices Code of Practice on the Information Commissioner's roles and responsibilities.

16.10 The Act requires that the Information Commissioner provides independent oversight of the integrity, security or destruction of data retained by virtue of Part 4 of the Act. Data is retained by virtue of Part 4 where the retention of that data is specifically required by a retention notice. There will be circumstances where the data might be stored in different systems across a Communications Service Provider's network, for example for business purposes as well as in a dedicated retention store. In such circumstances, the ICO must audit any system that the TO or PO uses to comply with the retention requirements in a data retention notice.

16.11 Where data is retained as a consequence of a data retention notice, but the TO or PO has a lawful reason to move or copy the data to a separate store, data retained in the separate store, insofar as it is no longer being retained in order to comply with a retention notice, is not subject to audit by the Information Commissioner under the Act. These circumstances may include where a copy of retained data that has been disclosed under Part 3 of the Act is being kept in the event of later challenge in court, see paragraph 15.12. Such data must still be kept securely and will be subject to relevant data protection legislation. However, it is not subject to audit by the Information Commissioner under the Act because the lawful basis for retaining the data will no longer be a retention notice, instead the Information Commissioner's regulatory powers under the data protection legislation may be applicable.

16.12 Where data retained under a retention notice is moved to another store and kept for a separate lawful purpose, details of the lawful basis for moving the data and keeping it in a separate store, along with details of the process used, must be kept by the TO or PO and provided to the Information Commissioner on request. This is to ensure that

the Information Commissioner can determine that any processes for accessing retained data comply with the security requirements.

16.13 This Code does not cover the exercise of the Information Commissioner's functions. It is the duty of any TO or PO subject to a notice under the Act to comply with any requests made by the Commissioner, in order to provide any information required by the Commissioner to discharge their functions. The Commissioner may, for example, make requests:

- to access any relevant premises;
- for copies of relevant documentation;
- to inspect any relevant equipment or other material; or
- to observe the processing of relevant CD.

16.14 Without prejudice to the independence of the Information Commissioner, a TO or PO may discuss a request from the Commissioner and its potential implications with the Home Office.

16.15 Reports made by the Information Commissioner concerning the inspection of TOs and POs and the security, integrity and destruction of CD retained under the Act may be made available by the Information Commissioner to the Home Office. This can help to promote good practice and identify security enhancements and training requirements within TOs and POs. The Home Office will work with TOs and POs to address any recommendations made by the Information Commissioner.

16.16 Subject to discussion between the Information Commissioner and the Home Office, either may publish the inspection reports, in full or in summary, or a single overarching report to demonstrate both the oversight of the security, integrity and destruction of data and TOs' and POs' compliance with the Act. Because of the sensitivity of identifying which companies have received retention notices, any such report must be sufficiently redacted to protect the identities of the companies.

16.17 Section 95(3) of the Act prohibits the Information Commissioner or a member of his staff disclosing the existence of a retention notice or the content of the retention notice to any person without the permission of the Secretary of State. However, this does not prevent the ICO from discussing a retention notice with IPCO as IPCO will, by virtue of their function in approving the notice, will already be aware of its existence and content.

Enforcement of integrity, destruction and security standards

16.18 The Act imposes a duty on TOs and POs to comply with requirements or restrictions imposed by the Act or a retention notice issued under the Act (see Chapter 5 in Notices Code of Practice). That duty is enforceable by civil proceedings brought by the Secretary of State.

16.19 In the event of a failure to comply with the integrity, destruction and security requirements contained in the Act or in a retention notice, the Secretary of State will consider whether enforcement action is appropriate or whether to work with TOs and POs to address any issues identified in the first instance.

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

16.21 Should the Information Commissioner identify any errors or issues relating to the disclosure of CD they may take such steps as they consider necessary to bring them to the attention of the TO or PO. Chapter 15 of this Code sets out the requirements on TOs and POs in relation to any such errors.

17 Contacts / Complaints

General enquiries relating to communications data retention and acquisition

17.1 The Home Office is responsible for policy and legislation regarding CD acquisition and disclosure. Any queries should be raised by contacting:

By post
Communications Data Policy Team
Investigatory Powers Unit
Home Office
2 Marsham Street
London
SW1P 4DF

By email
IPUCommunicationsData@homeoffice.gov.uk

Complaints

Data security, integrity and destruction

17.2 The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with the Act. Failure to comply with this Code's provisions in these areas may also engage concerns about compliance with data protection and related legislation. Any concerns about compliance with data protection and related legislation should be passed to the Information Commissioner's Office ('ICO') at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

0303 123 1113

www.ico.org.uk

Acquisition and retention of communications data

17.3 The Investigatory Powers Tribunal ('IPT') has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers, including those covered by this Code, as well as conduct by or on behalf of any of the intelligence services and is the only appropriate tribunal for human rights claims against the

intelligence agencies. Any complaints about the use of powers as described in this Code should be directed to the IPT.

17.4 The IPT is entirely independent from His Majesty's Government and the public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint or claim from a person, the IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination. A 'person' for these purposes includes any organisation and any association or combination of persons (see section 81(1) of RIPA), as well as an individual.

17.5 This Code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: https://investigatorypowerstribunal.org.uk. Alternatively, information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

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

This Code of Practice relates to the powers and duties conferred or imposed under Parts 3 and 4 of the Investigatory Powers Act 2016 relating to the acquisition of CD by public authorities and its disclosure by TOs and POs, and to the retention of CD by such operators.

It provides guidance on:

- procedures to be followed for the acquisition of CD;
- rules for the granting of authorisations to acquire data and the giving of notices to require disclosure of data;
- procedures to be followed for the retention of CD;
- security principles which must be adhered to by those retaining data;
- keeping of records, including records of errors; and
- the oversight arrangements in place for acquisition and retention of CD.

This Code is aimed at:

- members of public authorities who are involved in the acquisition of CD whether as an applicant, a single point of contact, a designated senior officer or a senior responsible officer; and
- staff within TOs and POs who are involved in the lawful disclosure of CD or who currently, or may in the future, retain data under the Act.

Annex A: Communications Data Acronyms

AGPS	Assisted Global Positioning System
BSSID	Basic Service Set Identifier
CD	Communications Data
CD SPoC	Communications Data Single Point of Contact
CEMA	Customs and Excise Management Act 1979
CPIA	Criminal Procedure and Investigations Act 1996
DNS	Domain Name System
DSO	Designated Senior Officer
FQDN	Fully Qualified Domain Name
GDPR	General Data Protection Regulation
GPS	Global Positioning System
IC	Information Commissioner
ICO	Information Commissioner's Office
ICR	Internet Connection Record
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPA	Investigatory Powers Act 2016
IP(A)A	Investigatory Powers (Amendment) Act 2024
IPAR	Internet Protocol Address Resolution
IPC	Investigatory Powers Commissioner
IPCO	Investigatory Powers Commissioner's Office
IPT	Investigatory Powers Tribunal
KYC	Know Your Customer
MSISDN	Mobile Station International Subscriber Directory Number
MLA	Mutual Legal Assistance
NAFN	National Anti-Fraud Network
NCA	National Crime Agency
NPCC	National Police Chiefs' Council
NPG	National Prioritisation Grades
OTO	Overseas Telecommunication Operator
PQDN	Partially Qualified Domain Name
PO	Postal Operators
PUK	Personal Unlocking Key
RIPA	Regulation of Investigatory Powers Act 2000
SRO	Senior Responsible Officer
TILEDG	Telecommunications and Law Enforcement Development Group
TO	Telecommunications Operators

Annex B: Communications Data Decision Making Flowchart

A Flow Chart has been created which will assist applicants and Accredited Communications Data Single Point of Contacts in the decision-making process of CD acquisition.

Where an applicant or Accredited CD SPoC is considering the meaning of any word used, they are strongly advised to refer to the original text in the Act, and associated definitions where available, or seek legal advice.

[Add link here]

Annex C: Communications Data Operational Examples

This annex provides operational examples to assist in the decision-making process, therefore, should be read and applied in parallel to the information outlined within this Code and Act.

Payment data and banking services

1. Online banking data, such as the IP address used by the customer to enable a transfer of funds, is CD. This is because the IP address associated with the transfer event, and the date and time of the online access to make the transfer, relate to the 'use' of the telecommunication service. The detail of the transfer itself, such as who money was sent to and how much, will not be CD as this relates to the content of communication.

2. The data generated from Payment Solution Providers, which is data that relates to mobile phone top ups, is CD as this type of data enables access, and therefore relates to the provision of the telecommunications service or system.

3. A bank statement with the name and address of the customer and the name of the payee, or location or store number of the merchant concerned in the transaction, is not CD. As a result, the data cannot be obtained using a Part 3 authorisation.

4. Card activity regarding financial transactions undertaken in person will not be CD. Where a card payment is made online – some data, including the IP address associated with the transaction, together with date and time of the related access, will be CD and require a Part 3 or other lawful authority to enable its disclosure by compulsion.

5. Transaction data that includes identifiable detail in the payment reference, such as when a payment to the DVLA includes a vehicle's registration in the payment reference, would be content data and therefore not covered under the scope of CD.

Further information can be found at: https://assets.publishing.service.gov.uk/media/649e843145b6a200123d45ad/REDACTED_Guidance_on_Definition_of_Communications_Data.pdf . The information within the 'Definition of CD' Quick reference is also included within the main body of this Code throughout the relevant sections.

Annex D: Prioritisation of Enquiries

1. This annex covers the prioritisation and grading that should be applied to Communications Data (CD) enquiries. For the purpose of this annex, the following definitions apply:
    - **Grade** refers to the Telecommunications and Law Enforcement Development Group ('TILEDG') National Prioritisation Grades ('NPG') used by TOs. More information on the grading can be found at paragraph 8.
    - **Priority** refers to the Investigatory Powers Commissioners Office ('IPCO') Authorisations Prioritisation Grades. More information on the prioritisation can be found at paragraph 12.

2. Given the implications of a significant volume of Grade 2 and Priority 2 requests, and the availability of specialist support, the guardian and gatekeeper role of the Communications Data Single Point of Contact (CD SPoC) is paramount; particularly as the handling of Grade 2 requests by Telecommunications Operators (TOs) increasingly involves complexity, where required information necessitates the need for specialist support (particularly outside office hours) and the handling of Priority 2 requests to IPCO Authorisations impacts all CD SPoC teams.

3. The CD SPoC is independent of the investigation and should determine the NPG and IPCO priority independently of the investigator and of any local policy in force at the time of the application, to ensure limited resources are arranged in a way which is equitable to the entirety of the Requesting Authority community, IPCO Authorisations and the TOs.

4. The IPCO Authorisations priority and NPG grade shall be considered by the CD SPoC independently of one another, as each system serves a different purpose. The assignment of the priority and grade in respect of each specific application for CD are the responsibility of the CD SPoC alone, as part of the guardian and gatekeeper role.

5. Overuse of Priority 2 impacts applications that have been correctly prioritised, as well as IPCO Authorisations' capacity for handling Priority 3 and 4 applications within Service Level Expectations (SLE). The over-prioritisation to Priority 2 by one Force or Authority also impacts on the CD application handling time for all other Forces and Authorities as IPCO Authorising Individuals will subsequently focus on those over-prioritised applications at the detriment to all other CD applications received at the same time. The use of IPCO Authorisations Prioritisation Grading can be subject to IPCO inspection and oversight.

6. The TOs also have limited personnel resources making it essential that these resources are utilised in a way that is equitable for all parties, making it essential that incoming requests are properly graded, according to the nationally agreed priority-grading systems.

7. The CD SPoC should note that an NPG Grade 2 is not the same in terms of requirement and processing as an IPCO Authorisations Priority 2 which aligns to IPCO SLEs. The CD SPoC should independently consider both the IPCO priority to attach to a CD application to IPCO Authorisations which may or may not then have the same grading requirement in submission to the TO. It may well be that an NPG grading could be higher or lower than that included on the CD application submitted to IPCO AIs for consideration. This will be determined by operational requirement, including operational resources deployed or readily-deployable. Both sets of prioritisation and grades are set out in the tables below.

IPCO Authorisations Priorities

8. The IPCO Authorisations Priorities includes four priorities which IPCO Authorisations have set SLEs for turning around CD applications.

IPCO Authorisations Priorities		
	Definition	**Service Level Expectation**
Priority 1	An immediate threat to life or national security - for exceptionally urgent applications which will not be submitted to IPCO. These will be authorised within the public authorities under the urgency arrangements set out in the Investigatory Powers Act section 61(a). These authorisations will be inspected by IPCO, post hoc.	N/A
Priority 2	Urgent operational necessity, or threat to life/national security not requiring immediate action - for where there is an urgent operational need for CD to: • assist in the prevention or detection of a serious crime; • make an arrest or seize illicit materials; or • ensure an operational opportunity is not lost.	6 working hours
Priority 3	Time critical enquiry - for matters that are not urgent but involve specific time-critical elements e.g. • bail dates; • court dates; • where persons are in custody; or	1 working day (15 working hours)

	• where timely acquisition of CD will assist in an investigation.	
Priority 4	Not a time critical enquiry - for everything else not covered above. e.g., where CD will assist in a legitimate investigation, but there is no urgency or time pressure to acquire the data.	6 working days

National Prioritisation Grades (NPG)

9. Public authorities, IPCO, TOs and POs may agree to the use of standards to indicate the appropriate timeliness for the response to lawful requirements for the disclosure of CD, such as the Telecommunications Industry Law Enforcement Development Group (TILEDG) grading scheme. This scheme uses three grades. The timescales attached to each grade are not service level agreements, and the time taken by a TO to respond to a request will depend upon multiple factors, including the nature and complexity of the request, and the manner in which it is submitted.

National Prioritisation Grades (NPG)		
	Definition	**Timescale** (begins when the TO becomes aware of the requirement)
Grade 1	An immediate threat to life	As soon as possible, but ideally within 30 mins (automated) or 60 mins (manual)
Grade 2	Exceptionally urgent requirement for the prevention or detection of serious crime; a credible and immediate threat to national security; or, a serious concern for the welfare of a vulnerable person where urgent provision of the communications data will have an immediate and positive impact on the investigation or operation	As soon as possible, but ideally within two hours (automated) or two working days (manual) [For the present purpose, the UK working week is defined as Mon-Fri, 09:00-17:00 and excludes Bank Holidays].
Grade 3	All other enquiries; but, where appropriate, will include specific or time-critical issues. For example, bail dates; court dates; where persons are in custody; or where there is a specific line of investigation into a serious crime and early disclosure by the telecommunications operator or	Resolution by end-to-end electronic process: data to be disclosed as soon as possible, but ideally within two working days; resolution by (partly) manual process: data to be disclosed as soon as possible, but ideally within ten working days.

	postal operator will directly assist in the prevention or detection of that crime.	

10. Grade 1 resources can be deployed to help operational need where feasible and appropriate across all requests, such as Grade 2 requests where there may be serious concern for the welfare of a vulnerable person. The CD SPoC should consult the TO in these circumstances.

11. With Grade 1 and 2, the emphasis is on urgent provision of the CD in anticipation of an immediate and positive impact on the investigation or operation.

12. Realistic timescales for the disclosure of data lawfully acquired are regularly updated by TOs and are communicated from time to time.

Annex E: National Error Reduction Strategy 2023

This latest release of the ERS updates all pre-existing versions; and, whilst the primary focus remains on the accurate resolution of internet protocol addresses (IPAR), public authorities who engage in the lawful acquisition of communications data (CD) may wish to extend the use of this guidance to other forms of lawful CD acquisition.

Who	Action
SRO	The SRO is responsible for the identification of the cause(s) of errors and the implementation of process to prevent recurrences. CoP Para 4.10.
Investigator / SPoC	Enforcement action based on the result of a single IPAR should be a last resort. Every opportunity should be taken to resolve other associated identifiers within the source document i.e. other IP activity or verified email addresses / mobile phones.
Investigator / SPoC	Recognise the particular difficulties of single strand information where enquiries will be dealt with 'out of hours' – unless there is imminent life-threat or risk of contact offending (CSE/A) such enquiries should be dealt with during normal working hours
Investigator / SPoC	Recognise the enhanced risk of errors whenever the urgent oral process is used. Risks include the verbal passing of identifiers, lack of corroboration and latency of data reaching the event data record.
Investigator	Upon the receipt of any information an immediate check for errors should take place. In the case of CSE/A referrals this will be material downloaded from source systems
Investigator / SPoC SRO	Wherever possible the source document containing details of the IP to be resolved must be attached to the application. If no source document is available, the investigator must confirm the non-existence of a source document to the SPoC. SROs may wish to consider the submission of a supporting document to accompany applications for other identifiers i.e. MSISDN.
Investigator / SPoC	Investigator and SPoC will check, verify, and agree date format – UK dd/mm/yyyy **v** US mm/dd/yyyy
Investigator / SPoC	Avoid requesting data either around midnight, or at the end of a calendar month. These are easy ways to avoid common causes of error.
Investigator	Where possible all relevant identifiers alongside dates / times should all be copy / pasted (CTRL+C/CTRL+V) into an application. Confirming the method of transportation into the application is advised. If not possible, a second person must verify these details have been inputted correctly with the application suitably endorsed.
Investigator / SPoC	Where available lease times for the allocated IP should be sought.
Investigator / SPoC	Agree the most appropriate IP addresses to resolve where they have been acquired from an IP History result, to mitigate risk of transposition or TO errors. Where both fixed line and resolvable mobile IPs are available, both should be resolved to increase the opportunity to focus on the appropriate subject. Great care should be taken if the IP activity being resolved is within 24hrs of the start or end time of the relevant session,
Investigator	Multiple IP addresses should be grouped by relevant Telecommunications Operator (TO)

SPoC	**Peer Review (1)** A second SPoC (subject to SRO oversight and decision-making) should verify as accurate the time-zone, date/times, and IP address against the source document before sending to IPCO Authorisations.

Who	**Action**
SRO / SPoC	Finding errors at the peer review one prevents a reportable error. These so-called near misses should be recorded and be subject of internal review where learning can be identified and shared.
IPCO Authorisations	Authorising Officers shall return all IPAR applications if the following is missing or not explained: • no confirmation of Peer Review One being carried out. • where application seeks the resolution of a single IP address
Second SPoC	**Peer Review (2)** To verify as accurate the date/times and IP address being entered onto the TO portal / Notice before being sent / served.
SPoC	Importance of Peer Review 1 if CD is acquired via AA, as no Peer Review 2 is feasible.
SPoCs	**Peer Review (3)** A check is made before release to verify that the identifiers in the returned result match those contained in the application and source document.
SPoC	Recognise that when AA is used, the applicant may receive the result at the same time as the SPoC. Immediate contact by the SPoC to the applicant is vital if the SPoC Peer Review 3 identifies an error.
Investigator	A package for the consideration of enforcement action must include all pertinent checks in an effort to corroborate the result of the original IPAR. No executive action should be taken without adequate corroboration.
Supervisor	An investigation supervisor will review the package upon completion. This may be the last opportunity for potential errors to be identified before operational activity
Investigator	If non urgent package involving IPAR is forwarded to another organisation, ensure inclusion of source document and original CD application form.
Receiving LEA SRO / Investigator	The receiving LEA must ensure all documentation is present and reviewed before action is considered. Involvement of SPoC in this checking process is at the discretion of the SRO
Investigator / SPoC	Investigators must feedback to SPoCs any unexpected results. In turn, a near miss involving TO data should be discussed with KET to decide who is best placed to raise the issue with the TO (UK or Overseas).
Investigator / SPoC	Appreciating the difficulty where online investigation units are not co-located, it is important to ensure constant contact between investigators and SPoCs
Investigator / SPoC	Changes to CD services alongside IPCOs findings from error investigations can lead to publications upon CDS of the issue and measures to prevent a reoccurrence. These can be found by typing ERS into the search box. Awareness of these bulletins by all involved in the acquisition process is essential.