*Below are excerpts (in black) from the current CD Codes of Practice where section 261 is mentioned in ‘the composition of communications’. Section 2 will be amended to include the change in definition of communications data to include subscriber details. The proposed changes to text are in red.*

**Composition of communications**

**2.15** For the purposes of the Act communications may comprise two broad categories of data: systems data and content. Some communications may consist entirely of systems data and will not therefore contain any content. Section 261(6)(b) makes clear that anything which is systems data is, by definition, not content. Additionally, when permitted by the Act, certain data may also be separated from the remainder of a communication in circumstances where, if it were so separated, it would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication. This is identifying data. Systems data and identifying data may be obtained by interception or equipment interference warrants under Parts 2 and 5, and Chapters 1 and 3 of Part 6 of the Act. Further details on systems and identifying data can be found in the interception and equipment interference codes of practice.

**2.16** Communications data is a subset of systems data. The Act is clear that, even though systems data cannot be content, communications data is limited to data which does not reveal anything of what might reasonably be considered to be the meaning of the communication (but any meaning arising from the fact of the communication or transmission of the communication is not content). That is, any systems data which would, in the absence of section 261(6)(b), be content, cannot be communications data

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

**Communications data**

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

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

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

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

**Telecommunications definitions**

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

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

**2.23** This data includes information about any person or entity to whom a service is provided, whether a subscriber or guest user and whether or not they have ever used that service. For example, this may include information about the person associated with an email address even if that email address has not been used since its creation.

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

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

**2.26** For example, for a social networking provider data such as the status of the account, contact details for the customer and the date a person registered with the service would all be communications data as they relate to the use of the service. However, other data held by the provider about a customer which does not relate to the provision of the telecommunications service, including personal information such as political or religious interests included in profile information, is not within scope of the definition of communications data.

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

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

· identifies or assists in the identification of the sender or recipient of a communication or their location;

· identifies or assists in the identification of or selects the apparatus used to transmit the communication;

· Identifies or assists in the identification of the signals which activate the apparatus used (or which is to be used) to transmit the communication; and

· identifies or assists in the identification of data as being part of a communication.

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

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

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

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

**2.31** This element includes other information held by a telecommunications operator about the use of the service such as information that the provider holds for billing purposes.

**Data which is about the architecture of a telecommunication system**.

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

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

**Entity and Events Data**

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

· entity data – this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices);

· events data – events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

**2.35** The authorisation levels required to access communications data reflect the fact that the set of events data as a whole contains the more intrusive communications data, including information on who has been in communication with whom, a person’s location when their mobile device connects to the network and internet connection records. The rank of the designated senior officer that can authorise acquisition of data reflects the differing levels of intrusiveness of the data. For example, in certain circumstances, the police can authorise access to entity data at Inspector level, but events data is authorised at Superintendent level. Additionally, entity data can be obtained in a wider range of crime types than events data.

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

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

**Entity data**

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

**2.39** Examples of entity data include:

· ‘subscriber checks’ such as “who is the subscriber of phone number 01234 567 890?”, “who is the account holder of e-mail account example@example.co.uk?” or “who is entitled to post to web space [www.example.co.uk](http://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,

· information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services,

· information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and

· information about selection of preferential numbers or discount calls.

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

**2.41** Some telecommunications operators may choose to retain user passwords as clear text for business purposes. In this context passwords would constitute entity data. Any information, such as a password, giving access to the content of any stored communications or access to the use of a communications service may only be sought under Part 3 of the Act from a telecommunications operator in the following circumstances:

 · where such information is necessary in the interests of national security; or

· for preventing death, injury or damage to health.

**2.42** A communications data authorisation cannot authorise a public authority to use a password obtained through that or another communications data authorisation. If a public authority wishes to use a password obtained through a communications data authorisation to access the content of stored communications or any communications service it must, in accordance with section 6

**2.43** of the Act, ensure that it has appropriate lawful authority.

**Events- paragraphs 2.44 to 2.45 remain the same**

**Postal definitions- paragraphs 2.46 to 2.53 remain the same**

**Content**

**Telecommunications definitions**

**2.54** 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.

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

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

**2.57** There are three exceptions to the definition of content (set out in section 261 (5) and 261 (6)). The first exception at 261 (5A) is in the context of the submission of online forms. The details included in these forms when they are submitted could be considered the “meaning” of that communication with the telecommunications operator or service provider. However, amendments brought forward in the Investigatory Powers (Amendment) Act 2024 make clear that this type of entity data will be communications data as it is about an entity to which a telecommunications service is provided and identifies or assists in identifying that entity or the location of that entity. For example, when seeking to identify the driver of a hire car the driver’s name and address details made via an online booking form will be communications data and not content. In this example the hire company is providing the telecommunications ‘service’ used to book the hire car. Public authorities are expected to apply for an IPA part 3 if they are unable to determine whether the communications data has been provided online or in person by a company representative and entered into an electronic system manually.

**X.X.** The second 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 communications data associated with the communication remains communications data and the fact that some meaning can be inferred from it does not make it content.

**X.X**. The third exception at 261 (6) (b) makes clear that systems data cannot be content.