*Below are excerpts (in black) from the current CD Codes of Practice where Internet Connection Records are mentioned. This primarily concerns Sections 2 and 9. Section 2 will require minor amendment to include the changes to the definition of third-party data as detailed within s87(4) of the Act and specific to Retention Notices. Most of the amendments are covered in an addition to Section 9 and the inclusion of a new sub heading and associated paragraphs specific to Condition D. The proposed changes to text are in red.*

Restrictions in relation to Condition D for Internet Connection Records.

2.74 An internet connection record (‘ICR’) is a record of an event held by a

telecommunications operator about the service to which a customer has connected on the internet. An ICR is communications data which may be used to identify, or

assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or program where that data is generated or

processed by a telecommunications operator in the process of supplying the

telecommunications service to the sender of the communication. In many cases

ICRs will be held by internet access providers, which are telecommunications operators which provide access to the internet and can include a home broadband connection, mobile internet or publicly available Wi-Fi.

2.75 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.

2.76 There is no single set of data that constitutes an ICR, as it will depend on the

service and service provider concerned. The core information that is likely to be

included is:

* a customer account reference – this may be an account number or an identifier of the customer’s device or internet connection,
* the source IP address and port;
* the destination IP address and port – this is the address to which the person is routed on the internet and could be considered as equivalent to a dialled telephone number. The port additionally provides an indication of the type of

service (for example website, email server, file sharing service, etc.) although

ports are often reused for different purposes; and the date/time of the start and end of the event or its duration.

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

* the volume of data transferred in either, or both, directions;
* the name of the internet service or attributable server that has been connected to; and
* those elements of a URL which constitute communications data – see paragraphs 2.60 to 2.67.

2.78 Where a data retention notice is considered which would require a

telecommunications operator to retain ICRs the specific data that an internet access provider may be required to retain will be discussed with the provider before the

requirement is imposed (Footnote 15).

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

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

*(Section 9 references to Internet Connection Records)*

Considerations in relation to the acquisition of internet data

Internet connection records

9.1 Under certain circumstances, an authorising individual may grant an authorisation to obtain data which constitutes or requires the processing or disclosure of an

internet connection record (ICR) (see paragraph 2.73 for the definition of an ICR).

Subject to paragraph 2.36 any application that involves the disclosure of ICRs must be authorised as events data.

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

involved.

9.3 Section 62 of the Act recognises the additional sensitivities associated with ICRs and restricts public authority access accordingly. A public authority can therefore

only require the disclosure or processing of internet connection records under Part

3 for the purpose of identifying:

* the user of an internet service (either the person or apparatus);
* the internet communications services (Footnote 49) a device or person is using, such as messaging applications;
* the internet services a device or person is using which wholly or mainly involve making available or acquiring material, whose possession is a crime – for example child abuse imagery or illicit drugs; or
* other internet services a device or person is using – for example to book travel or look at online mapping services.

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

purposes’.

9.5 The Act applies important restrictions when the statutory purpose for which ICRs

are acquired is “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, even if the only data to be acquired is entity data. There are further restrictions to the statutory purposes available for Condition D (see below).

9.6 The crime threshold does not apply to entity data applications made for the

investigative purpose of identifying the sender of an online communication (section 62(3)). Such applications will not result in the disclosure of a list of internet connection records as the service used will already be known. A telecommunications operator could be asked a number of different questions, for example who was using an IP address at a particular date/time, which of its customers accessed this server at a particular date/time or which of its customers conducted an activity of concern on a known website at a known date or time. Known in the context of conditions A, B or C means unequivocal, certain knowledge of a connection to a particular service during a particular date/time. The material disclosed will thus take the form of an IP address and related entity data, where available (see identifying the sender of an online communication in the next section). Should a request for this investigative purpose require the disclosure of any events data, however, the serious crime threshold will apply.

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

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

9.8 Such applications will require a telecommunications operator to disclose a list of

internet connection records covering a specific time period. This may include ICRs not directly relevant to the investigation. Given the scope for collateral intrusion the

authorising individual will therefore need to apply careful consideration to ensure this period is proportionate and no longer than necessary.

9.9 Occasions when a public authority might seek ICRs to identify an internet communications service being used include (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 identify who a person has been communicating with online or when they have been communicating. In most cases it will simply identify the

services which a person has accessed allowing further enquiries to be made of the

relevant provider.

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

viewing illegal images has been accessing sites containing this information, to

identify whether a person suspected of owning illegal weapons has been accessing online market places which wholly or mainly sell illegal items or to identify to which

website a person has uploaded illegal images.

9.12 A public authority might seek ICRs in relation to internet services more generally when seeking, for instance, to identify how and when a person who is suspected of

people trafficking is making travel arrangements or to identify any activity which may assist in locating a missing vulnerable person. Any services accessed by an

individual may provide leads for public authorities to pursue in their investigation by

identifying travel services, mapping applications or other relevant avenues to follow

up.

9.13 A public authority may only examine internet connection records returned to them which do not directly relate to the purpose for which they were acquired (for

example a record of access to a travel site returned in response to a request for

communication services) where necessary and proportionate to do so for the

purposes set out in section 60A(7), 61(7) and 61A(7) of the Act. For further

information see paragraphs 24.38 – 24.40 on excess data.

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

9.15 There may be circumstances where it is more appropriate for public authorities to utilise the alternative lawful powers available to them, such as interception or

equipment interference warrants, to obtain information, which is similar to, or

includes, ICRs. The use of these powers will be subject to higher levels of

authorisation. For example, a warrant must be issued by the Secretary of State and

approved by a Judicial Commissioner. Before using such powers, the relevant

authority must consider whether a less intrusive means of acquiring the data is appropriate.

--------------

*Proposed addition to Section 9*

Restrictions in relation to Condition D for Internet Connection Records

The Investigatory Powers (Amendment) Act 2024 introduced a further Condition D in respect of Internet Connection Records. This Condition relates to the use of ICRs for target detection purposes.

Condition A in the Act 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. Conversely, Condition D allows for situations where the adversary is assessed to be utilising one or more services in a given time period by removing 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.

For example, where 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, then a Condition A authorisation would be appropriate to identify the offender based on the known factors of ‘service’ and ‘date/time of use.’

However, where forensic examination of a seized device identifies a website hosting illegal images of children, and investigators wish to identify individuals who are accessing those resources, a Condition D authorisation would be appropriate. This is because they have reasonable belief that individuals are accessing the illegal content but lack the requisite unequivocal knowledge for a Condition A authorisation.

However, use of this new Condition D;

* is limited to the United Kingdom Intelligence Community (UKIC) and the National Crime Agency (NCA) only. These agencies should ensure they have an understanding of the construct of the ICR data, appreciation of human versus machine generated connections, and understanding of computer logic and the importance of accurate syntax. Other Public Authorities are not permitted to seek access to ICRs under Condition D.
* is limited to ‘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 serious crime purposes. Serious crime is defined at section 86(2A) of the Act, and, for UKIC, 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 still meet necessity, proportionality and collateral intrusion tests. The applicant must explain their reasoning with reference to tangible supporting information, including (where appropriate) their subject matter expertise and analysis.
* 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. These Codes of Practice are unequivocal on this point, stating at 3.14; “*When granting an authorisation, the authorising individual must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual’s rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest*.”
* requires that applicants also 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 this Condition will necessarily be more subjective in nature. The need to address collateral intrusion is particularly important where the services concerned are otherwise innocent in nature, as per the above legitimate video conferencing facility, but also applies where sites are illegal in nature, such as those promoting terrorism, child abuse or malware distribution, where some accesses may concern academic or journalistic research, or otherwise be innocent or 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.
* will be subject to oversight and reporting by the Investigatory Powers Commissioners Office.

------------------

*The below section is included for completeness as there is mention of ICRs therein. However, it is not envisaged that any changes are required to these paragraphs.*

**Identifying the sender of an online communication**

9.16 Internet protocol address resolution (IPAR) is necessary to identify the sender of an online communication, where the public authority is in possession of a source IP address related to a communication of interest and needs to determine the customer linked to this address. There is often a pressing need for such requests to

identify individuals online, for example in terrorism and child abuse investigations. In

the current technological environment this is often not a simple task and

applications to acquire communications data for this purpose must consider the

associated complexities and balance these against the operational requirements.

9.17 In order to communicate on the internet a device must be allocated an IP address.

A communication may be:

* between two users, in which case the IP address will normally relate to their

personal electronic device, or to the internet access point to which their device is connected;

* between two servers in which case the IP addresses will relate to the equipment in question;
* or between a user’s personal electronic device and a server, for instance a user downloading material from a website.

9.18 The implementation of network address translation and dynamic IP addressing means that an IP address may only be allocated to a particular user in conjunction

with other users, and sometimes for an extremely short period of time, particularly

where allocated to mobile devices. In most cases, the IP address from which the

communication originated is the source IP address, and the address by which it is

received is the destination IP address (Footnote 51).

9.19 In order to enable the telecommunications operator to resolve a source IP address to a customer the public authority must provide a minimum of one source IP

address and one date/time or range of time. To enable the identification of a person

who initiated a communication, rather than the service used to send that communication, this must be a source IP which relates to a specific device operated by an individual, not to a destination device (e.g., a server).

9.20 However, where IP addresses are shared between network customers, providing

just the source IP address and the time of the communication will often not be

sufficient for a telecommunications operator to resolve the address to an individual

customer. Public authorities should therefore ensure they include any other data

that is available to them with the application. For example, if there are more IP

addresses and times (or time ranges) which they believe relate to the same device

or person then that data should also be provided to the telecommunications

operator. Other examples of data types include:

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

9.21 Where public authorities need to resolve IP addresses, internet connection record data will frequently be the only additional data that is available. This is because they will already know the internet service that has been used by the device or person which they are trying to resolve. For example, if someone posts a bomb threat to an online blog, the blog’s access records may provide the police with both the source IP address allocated to the user who posted the threat, and details about the server hosting the blog, such as the IP address of the server. In such circumstances, the police should provide both these IP addresses, plus any other information the blog records provide such as port numbers used, to the telecommunications operator as this will increase the likelihood that the telecommunications operator will be able to accurately match these details to an individual customer. (Footnote 52)

9.22 Where a public authority provides internet connection record data, such as a

destination IP address, to a telecommunications operator in order to resolve a

source IP address, that request will require the telecommunications operator to

process internet connection records. It will therefore be considered under Condition

A in section 62 concerning restrictions in relation to internet connection records.

Where the public authority is aware that the telecommunications operator allocates

multiple customers the same IP address then, where possible, the internet

Footnote 51

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

Footnote 52

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

connection record data should be provided by the public authority to the

telecommunications operator. (Footnote 53)

9.23 In cases where an IP address may only be allocated to a particular user in

conjunction with other users, an authorisation for IPAR data may return a large data

set to the public authority. As an authorising individual may not know in advance

how large that return will be, it is important to consider the proportionality and

potential collateral intrusion of such applications.

9.24 In addition to the standard authorisation procedure for communications data

applications the following additional steps should be taken when seeking to identify

the sender of an online communication:

* the applicant should consider what data is available to them and base their

application on those elements of data which will enable the telecommunications

operator to make the most appropriate and proportionate return;

* the applicant should use as many relevant identifiers as are available to them in making their application, in order to ensure that the telecommunications operator may make the most appropriate return. Where more than one IP address or more than one date / time is available, the public authority should consider resolving more than one to allow cross-correlation of data sets;
* the authorising individual must take account of advice provided by the SPoC as to an appropriate strategy for the acquisition of IPAR data in each case;
* The authorising individual should consider whether to specify that data should

only be returned where it can be linked to one individual or whether larger data sets may be returned. The authorising individual may decide to accept returns of larger data sets only where the necessity and proportionality case is sufficiently strong and must detail their considerations of proportionality in the authorisation;

* if the SPoC considers that data may be returned that links to more than one

individual, they must, though consultation with the telecommunications operator, provide the authorising individual with guidance as to the amount of data that is likely to be disclosed; and

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

Footnote 53 The telecommunications operator may disclose the internet connection record data back to the public authority when it discloses the user of the source IP address in question (see paragraph 2.37 for further details on where a telecommunications operator may disclose data originally provided by the public authority).

9.25 The considerations above will also apply to authorisations where the public authority does not have an IP address but wishes to determine the individual that carried out a certain action online. For example, if a public authority suspects an

internet service is being used to share child abuse imagery it may be appropriate to

determine all users of the service over the specified timeframe.