Criminal Cases Review Commission

CASEWORK POLICY

Policy Title: **Accessing Telecommunications Data**
Reference: **CW-POL-17** Version: **1.0**

Contents

The CCRC's Quality Statement

The CCRC is committed to achieving high-quality case reviews as quickly as possible. In order to achieve this, we operate under a Quality Management System; please see 'Q-POL-01 CCRC Quality Policy' for further information. Our policy documents are available on our website: www.ccrc.gov.uk.

If you or someone you represent has difficulty accessing the internet then please contact us via 0300 456 2669 (calls charged at local rate) and we will send a hardcopy of the relevant policy free of charge.

This is a quality-controlled document. Significant changes from the last issue are in grey highlight: like this. Significant deletions are shown as: [text deleted].

Introduction

This policy explains how the CCRC accesses telecommunications data. It also states the nature of the data that can, and cannot, be obtained by the CCRC.

Key Points

1) The CCRC's accessing of communications data in the course of a review is strictly regulated by law.

2) The CCRC can use its legal powers to obtain communications data that has already been obtained and retained by a public body.

3) Although the CCRC can use its legal powers to obtain material from the private sector, the CCRC cannot use those powers to obtain communications data and must instead use RIPA or IPA.

4) The CCRC is Relevant Public Bodies authorised to obtain communications data for the investigation of a miscarriage of justice.

5) Communications data **does not include any material that forms the content** of a communication (e.g. what was said in a phone call, contained within a text message or contained within an email).

6) Communications data is the context (e.g. which phone number was communicating; when; and with which other phone number).

7) The contents of communications and when they may be lawfully intercepted is strictly governed under Section 4 of the IPA - the CCRC has no involvement with this.

Definitions

Key Word	Meaning
CAA	Criminal Appeal Act 1995
CSP	Communications Service Provider
DSO	Designated Senior Officer
ICR	Internet Connections Record
IPA	Investigatory Powers Act 2016
IPCO	Investigatory Powers Commissioner's Office
OCDA	Office for Communications Data Authorisations
RPB	Relevant Public Body
SPoC	Single Point of Contact
URN	Unique Reference Number

---

1 Background Information

1.1 The communications industry in the United Kingdom is entirely managed by the private sector and the CCRC's accessing of communications data in the course of a review is strictly regulated by the Investigatory Powers Act 2016 (IPA) and its accompanying Codes of Practice.

1.2 The CCRC can use its legal powers under section 17 of the Criminal Appeal Act 1995 (CAA) to obtain communications data that has already been obtained and retained by a public body in the course of an investigation / prosecution but the CCRC **cannot obtain new** material outside of the IPA.

1.3 Similarly, although the CCRC can use its legal powers under section 18A of the CAA to obtain material from the private sector, the CCRC cannot use those powers to obtain communications data and must instead use the IPA.

1.4 The IPA prescribes the specified purposes for, and process of, obtaining communications data and the Relevant Public Bodies (RPBs) empowered to obtain that data. The CCRC is an RPB under section 70 of the IPA which specifies the CCRC as an authorised body which can obtain data for the investigation of a miscarriage of justice.

1.5 The IPA specifies "communications data" rather than telecommunications data. Under the IPA, communications data is not confined to telecommunications data and includes postal, telephone, and Internet Connections Records (ICRs).

1.6 Communications Service Providers (CSPs) provide communications services. Strictly regulated arrangements exist with CSPs for the retention and provision of data to RPBs.

2 Telecommunications Data

2.1 The focus for the CCRC in this policy is telecommunications data (i.e. communication that is carried out using a telephone or the internet). However, obtaining data from a CSP providing postal communications follows the same process stated in this policy.

2.2 Telecommunications data falls into two new broad categories:

I. **Entity Data**
For example:
- Subscriber details, including the name and address of the subscriber of a phone number or the account holder of an email address.

II. **Events Data**
For example:
- Itemised billing
- Traffic data (e.g. cell site (location) analysis, or records of calls made to and from a phone number in a particular period, often colloquially referred to in criminal investigations as 'AB' or 'in/out data').
- Internet Connection Records (ICRs) provide details of the internet service that a specific device has connected to e.g. a website or instant messaging application). It does not provide full browser histories or details of every web page visited, content of an Instant Message or details of a message recipient, or any activity of a particular website.

2.3 Communications data **does not include any material that forms the content** of a communication (e.g. what was said in a phone call, written within a text message or contained within an email).

2.4 Communications data is the context (e.g. which phone number was communicating; when; and with which other phone number). It can include the duration of a communication.

2.5 This means that while the CCRC may be able to establish from a CSP that person "A" sent a text message to person "B", on a certain date at a certain time, the CCRC **cannot obtain the content** of the text message itself from the CSP under the IPA.[1]

[1] The contents of communications and when they may be lawfully intercepted is strictly governed under Section 4 of the IPA - the CCRC has no involvement with this.

3 Authorisation and Designated Roles

3.1 The IPA sets out designated roles within an RPB, they are as follows:

3.1.1 **Applicant**: This term is used in relation to the person making the request for the communications data. The CCRC will adopt the same term, but the documentation supporting the request for data will clearly differentiate between the person making the request and the person making an application to the CCRC for the review of their case. Any reference to the term 'applicant' in this policy applies to the person making the request for the data and not to the person applying to the CCRC for a review of their case.

3.1.2 **Single Point of Contact** (SPoC): The SPoC is an individual trained and formally accredited to facilitate the lawful acquisition of communications data and effective cooperation between an RPB and a CSP. Within the CCRC two members of staff are accredited and thus authorised to perform the SPoC function. **CSPs will not enter into any communication with anyone from an RPB other than an accredited individual**. All CSPs hold details of accredited individuals.

*N.B. Under **no circumstances** will anyone within the CCRC **other than a designated CCRC SPoC** make a direct approach to a CSP. Any such approach is reportable to the Investigatory Powers Commissioner.*

3.1.3 **Designated Senior Officer** (DSO): The DSO is responsible for the oversight and integrity of the process in place - compliance with the legislation and Codes of Practice; the recording and reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise errors or their repetition. In the relatively uncommon event that a CSP returns Excess Data, the DSO is required to review that data and to authorise its use if it is necessary and proportionate to do so.[2] The CCRC's DSO is the Director of Casework Operations.

[2] See Codes of Practice, 24.38 to 24.40.

4 CCRC Procedure and Recording Arrangements

4.1 It is essential that all matters relating to the acquisition of communications data are accurately and fully recorded. Records are subject to periodic audit by an inspector from the Investigatory Powers Commissioner's Office (IPCO).

4.2 All communications with a CSP will be recorded, including any contact to establish the likelihood of relevant data being available. An individual electronic SPoC Log will be maintained in each case. A copy of the SPoC Log will also be retained by the SPoC.

4.3 A Communications Data Application Form will be completed electronically. The SPoC will ensure each application has:

I. a Unique Reference Number (URN)
II. meets with the provisions of the IPA and associated Codes of Practice, and
III. will add to it any necessary comments, observations or recommendations for approval.

4.4 Applications are submitted electronically for independent authorisation by the Office for Communications Data Authorisations (OCDA). OCDA notifies the RPB whether it has authorised or rejected an application in the form of a Decision Document. The SPoC must retain records of both the communications data applications that they issue as well as the decisions received from OCDA.

4.5 If the Application for Communications Data is approved by OCDA, the SPoC will prepare the necessary Notice under IPA to be served on the CSP(s) concerned, generally by email. Responses will usually be received by the same means. A separate Notice is required for each request made and each Notice will have an individual URN.

4.6 Application Forms for Communications Data, Notices to CSPs and data provided to the CCRC by CSPs will, by their nature, contain sensitive and personal data and so they will be appropriately security marked and stored by the SPoC, in accordance with the CCRC's policies on Government Security Classification marking and handling of material.

5 The 'Golden Copy'

5.1 Any data provided to the CCRC by a CSP as a result of a request for data under the IPA must be retained. This material is referred to as the 'Golden Copy' and this will always be retained so it can be presented as evidence in any future legal proceedings (if required). This is necessary because the CSP may not itself retain the original data beyond the prescribed 12-month period.

6 Disclosure

6.1 All material will be retained and dealt with in accordance with the CCRC's policy on Government Security Classification Marking. All material will be subject to the CCRC policy 'CW-POL-19 Disclosure by the CCRC'.

7 New Offences under the IPA

7.1 Unlawfully obtaining communications data applies to anyone within a Public Authority. To be an offence, unlawfully obtaining or providing communications data must be done knowingly (i.e. acting voluntarily and intentionally) or recklessly (e.g. with obvious / foreseeable consequences). SPoCs will not have committed an offence simply for making a mistake.

7.2 This offence applies to anyone working directly or indirectly for the CSP and prohibits them from disclosing the existence of a communications data request. It is incumbent on the Applicant to make clear whether or not disclosure is permitted, as disclosing with the relevant Public Authority is a reasonable excuse to this offence.

Appendices
None

Relevant CCRC Documents

Q-MAN-01	CCRC Quality Manual
Q-POL-01	CCRC Quality Policy
CW-POL-19	Disclosure by the CCRC
#1662614	Government Security Classification Policy
#1897298	Handling Government Classified Information Policy

Legal Documents (available for free from www.legislation.gov.uk)
Criminal Appeal Act 1995
Investigatory Powers Act 2016

Document Control
Document author: Head of Investigations
Issue authorised by: Director of Casework Operations

Version History

Date Issued	Version	Brief Details of Change	DCR
15/07/2021	1.0	First Issue	21/04

*****END OF DOCUMENT*****