CCRC
Criminal • Cases • Review • Commission

ACCESSING TELECOMMUNICATIONS MATERIAL

FORMAL MEMORANDUM

Table of Contents

Background

1. The communications industry in the UK is entirely managed by the private sector and the Commission's accessing of communications data in the course of a review is strictly regulated by the Regulation of Investigatory Powers Act 2000 ("RIPA"), the Investigatory Powers Act 2016 ("IPA"), and any associated Codes of Practice. The Commission can under section 17 of the Criminal Appeal Act 1995 obtain from public bodies communications data that has already been obtained and retained by that public body in the course of an investigation/prosecution but the Commission cannot obtain new material outside of RIPA or IPA. In a like vein, while the Commission can obtain material from private bodies under section 18A of the Criminal Appeal Act 1995 it cannot use that power to obtain communications data and must use RIPA / IPA to do so.

2. The Investigatory Powers Act 2016 prescribes the specified purposes for, and process of, obtaining communications data and the 'Relevant Public Bodies' ("RPBs") empowered to obtain that data. The Commission is a RPB[1].

3. RIPA / IPA speak of "communications data", rather than telecommunications data. Communications data is not limited to telecommunications data, but includes it. Postal, telephone and internet communication is also caught by RIPA / IPA.

4. Communications Service Providers ("CSPs") provide communications services. Strictly regulated arrangements exist with CSPs (via in combination RIPA, the Data Retention and Investigatory Powers Act 2014, IPA, and any associated secondary legislation and Codes of Practice) for the CSPs to retain data and to provide it to RPBs.

Telecommunications Data

5. While "communications data" under RIPA / IPA includes postal communications, the focus for the Commission in this Memorandum is telecommunications data - i.e. that carried out by means of a telephone or the internet. Obtaining data from a CSP providing postal communications would follow that set out below for the acquisition of telecommunications data.

6. Telecommunications data falls into four categories, which, broadly, fall under the following headings:

   (i) Account information (e.g. subscriber details, including the name and address of the subscriber of a phone number or the account holder of an email address);

   (ii) Service use information (e.g. itemised billing);

   (iii) Traffic data (examples would be cell site 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');

   (iv) Internet and associated services.

[1] Section 70 of the Investigatory Powers Act prescribes the CCRC as an authorised body, and that it may obtain data for the statutory purpose of the investigation of a miscarriage of justice.

7. Communications data **does not include any material that amounts to the 'content'** of any communication – i.e. content is what was said in a phone call, contained within a text message or contained within an email.

8. 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.

9. That would mean, for example, that while a RPB may establish from a CSP that person "A" sent a text message to person "B", on a certain date at a certain time, the RPB **could not obtain the content** of the text message itself from the CSP under RIPA. The contents of communications and when they may be lawfully intercepted is strictly governed by a separate regime under Section 4 IPA - one in which the Commission has no involvement.

Authorisation and designated roles

10. RIPA / IPA set out designated roles within a RPB, they are as follows:

(i) **Applicant**: The term 'applicant' is used in relation to the person making the request for the communications data. The Commission 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 Commission for the review of his/her case. Any reference to the term 'applicant' in this Memorandum applies to the person making the request for the data and not to the person applying to the Commission for a review of their case.

(ii) **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 a RPB and a CSP.

(iii) Within the Commission at least one member of casework staff is accredited and thus authorised to perform the SPoC function as its designated SPoC. **CSPs will not enter into any communication with anyone from a RPB other than an accredited individual.** All CSPs hold details of accredited individuals.

(iv) Under **no circumstances will anyone within the Commission other than a designated Commission SPoC make a direct approach to a CSP. Any such approach is reportable to the Investigatory Powers Commissioner ("IPC")**.

(v) **Designated Senior Person** ("DP"): The DP is the person holding a prescribed office in a RPB who assesses the application for data, records his/her considerations of it and approves it if it is considered to meet the requirements of RIPA / IPA and allied Codes of Practice. The Head of Investigations is the only person prescribed by section 70 of IPA to act as a DP within the Commission.

(vi) **The Senior Responsible Officer** ("SRO"): The SRO 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. The Commission's SRO is the Director of Casework Operations.

Commission procedures and recording arrangements

11. 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").

12. 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.

13. A Communications Data Application Form will be completed electronically. The SPoC will ensure each application has a Unique Reference Number ("URN"), meets with the provisions of RIPA / IPA and associated Codes of Practice, and will add to it any necessary comments, observations or recommendations for the DP's consideration and approval. The DP will record his/her observations on the Communications Data Application Form and whether it has been approved or rejected. The SPoC will maintain a copy of the document generated at the conclusion of the process.

14. If the Application for Communications Data is approved by the DP, the SPoC will prepare the necessary Notice under RIPA which, after signature by the DP, the SPoC will serve 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.

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

The "Golden Copy"

16. Any data provided to the Commission by a CSP as a result of a request for data under RIPA must be retained. This material is referred to as the "Golden Copy" and this should always be retained so as to be capable of being adduced in 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.

Disclosure

17. All material will be retained and dealt with in accordance with the Commission's policy document on Government Security Classification Marking.

18. All material will be subject to the Commission's Disclosure Policy.