Acquisition and Disclosure of Communications Data

Guidance for the Layout of a Chapter II Application Form and Guidance for Applicants and Designated Persons Considering Necessity and Proportionality

HOME OFFICE
November 2007

DATA COMMUNICATIONS GROUP
November 2007

Introduction

This paper has been produced jointly by the Home Office and the Data Communications Group (DCG)*, in consultation with the Interception of Communications Commissioner's Office (IOCCO), to clarify what information should be included in an application for the acquisition of communications data in accordance with the Regulation of Investigatory Powers Act 2000 ("the Act") and the code of practice approved by Parliament under section 71 ("the code").

Where appropriate, the **GUIDANCE** set out in this paper should be included within a public authority's application process to assist applicants and designated persons.

The layout of this specimen document is for a paper based administration and has been prepared in **Microsoft Word 2002** using **Verdana** text.

Sections of the form can be amended to suit the working practice of the public authority whether managed on paper or on a database. However, changes must be in accordance with the Act and the code.

If you are viewing the specimen form in something other than Microsoft Word 2002, the colours and pagination may differ from the original.

*The Data Communications Group comprises representatives of ACPO, ACPO(S), HMRC, SOCA, other public authorities and senior members of communication service providers and their trade associations.

Application

An application, comments by the single point of contact (SPoC), considerations of the designated person, authorisations and notices may be made in writing ("paper") or electronically ("database").

Insert name of your public authority here

Chapter II of Part I of the Regulation of Investigatory Powers Act 2000

Application for Communications Data

1) Applicant's Name		**4) Unique Reference Number**	
2) Office, Rank or Position		**5) Applicant's Telephone Number**	
3) Applicant's Email Address		**6) Applicant's Fax Number**	

7) Operation Name (if applicable)		**8) STATUTORY PURPOSE**
		Click here for options:-

Subject to the restrictions upon public authorities, the Statutory Purposes for which communications data can be required are as follows (see paragraph 2.2 of the code);

- In the interests of National Security S22 (2)(a)
- For the prevention and detection of crime or preventing disorder S22 (2)(b)
- Economic well being of the United Kingdom S22 (2)(c)
- In the interests of public safety S22 (2)(d)
- For the purpose of protecting public health S22 (2)(e)
- For the purpose of assessing or collecting tax, duty levy or other imposition, contribution of charge payable to a government department S22 (2)(f)
- For the purpose, in an emergency, of preventing death or injury or damage to a persons physical or mental health or of mitigating any injury or damage to a persons physical or mental health S22 (2)(g)
- To assist investigations into alleged miscarriages of justice Article 2(a)
- For the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime Article 2(b)(i)

- For the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for his death or condition Article 2(b)(ii)

The police may use all the statutory purposes listed except for S22 (f) and Article 2(a).

Some of the statutory purposes have restrictions as to when it may be appropriate to use them (see footnotes 13, 14 and 15 of the code)

The drop down menu **STATUTORY PURPOSE** has been drafted for police use - other public authorities must amend the drop down menu appropriate to the statutory purposes permitted for their authority.

There is a restriction on the acquisition of communications data for S22 (d), S22 (e) & S22 (f). Only communications data within the meaning of S21 (4) (c) may be acquired for these purposes (see paragraph 2.3 and 2.4 of the code).

---

9) COMMUNICATIONS DATA **Describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s)**
This text box can be made bigger or smaller, it is not set out to indicate how much should be written

---

It may be appropriate for the section **COMMUNICATIONS DATA** to include 'text boxes' to enable the applicant to set out the:

- telephone number, email address, etc;
- where appropriate the 'between times / dates' of the data set required;
- type of data required, for example subscription details, outgoing calls, incoming calls.

An application may contain several requests for various 'data sets' relating to a specific investigation or operation. However, consideration should be given as to how this may affect the efficiency of the public authority's processes and the impact of managing disclosure issues before, during and after a criminal trial.

10) NECESSITY **State the nature of the investigation or operation and how it relates to a purpose at question 8** *Give a short explanation of the crime (or other purpose), the suspect, victim or witness and the phone or communications address and how all these three link together.*
This text box can be made bigger or smaller, it is not set out to indicate how much should be written

GUIDANCE

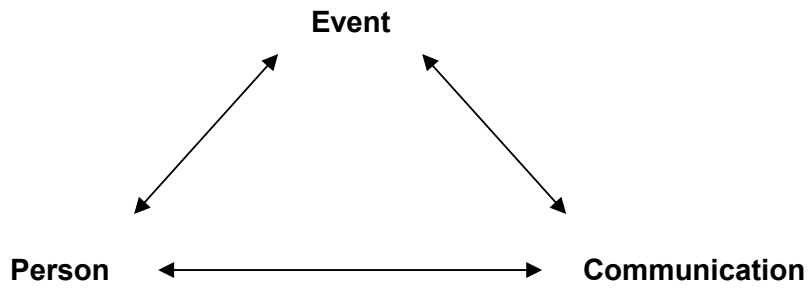
NECESSITY – In order to justify the application is necessary the applicant needs to cover three main points:

- crime / offence / circumstances ("the **event**") under investigation;
- suspect(s) / offender(s) / witness(es) / victim(s) ("the **person**") and how the person(s) is/are linked to the event;
- telephone number(s), IP Address(es) etc ("the **communication**") and how this/these relate or link the person and the event.

Sensitive sources of intelligence or covert investigation techniques may be referred to in the application but the applicant must be mindful of the appropriate security handling of the application once completed. It may be sufficient to refer to an intelligence reference number within the body application dependant on the security issues involved.

The information given by the applicant (which includes 'background information' or the 'intelligence case') should be set out within an application under the headings of **Necessity** and **Proportionality** (which includes the consideration of meaningful collateral intrusion). This will minimise the need to repeat information within an application and enable the process to be streamlined.

In essence, necessity should be a short explanation of the a) **event**, b) the **person** and c) the **communication** and how these three link together.



The applicant must establish a link (which may, where justified, include an inferential link) between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

A brief description of the investigation or operation may assist the designated person better understand the reason for the application.

In a long term or complex investigation or operation it is important to set the application in context with the overall investigation or operation and set the scene and background, which then leads into the applicant's specific investigative or operational requirements (which should be covered in the proportionality section).

Necessity does not entail explaining, 'what will be achieved by acquiring the data' or 'why specific time periods have been requested' – these points are relevant to proportionality and should be covered in the relevant section to stop repetition.

---

11) PROPORTIONALITY

State why obtaining the communications data is proportionate to what you are seeking to achieve

Outline what is expected to be achieved from obtaining the data and explain how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. When considering the benefits to the investigation or operation, can the level of intrusion be justified against the individual's right to privacy? Explain why you have requested the specific date/time periods i.e. how these are proportionate.

This text box can be made bigger or smaller, it is not set out to indicate how much should be written

12) COLLATERAL INTRUSION

Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances

If you have identified any meaningful degree of collateral intrusion, explain what it is.

This text box can be made bigger or smaller, it is not set out to indicate how much should be written

---

GUIDANCE

PROPORTIONALITY - Applicants should outline how obtaining the data will benefit the investigation or operation. The two basic questions:

- "What are you looking for within the data to be acquired?"
- "If the data contains what you are looking for, what will be your next course of action?"

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

An explanation as to how communications data will be used, once acquired, and how it will benefit the investigation or operation will enable the applicant to set out the basis of proportionality.

An investigation or operation which is seeking to acquire several sets of traffic data or service use data should engage with the SPoC to develop strategies (or collection plans) to obtain the communications data and the detail of that strategy may be included within the application (see paragraph 3.17 of the code).

COLLATERAL INTRUSION forms part of the **PROPORTIONALITY** considerations and becomes increasingly relevant when applying for traffic data or service use data and applicants should outline specifically what collateral intrusion may occur, how the time periods requested impact on the collateral intrusion, whether they are likely to obtain data which is outside the realm of their investigation and outline their plans for managing it, for example during the course of an investigation and to establish certain facts it may be necessary and proportionate for an investigator (applicant) to require access to communications data that relates to witnesses as well as the associates of a suspect or target.

The question to be asked is, "Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for? For example, due to the very specific nature of telephone subscriber check/s, collateral intrusion on a person other than the subscriber detail/s will be consistently absent whereas itemised billing on the subject's family home will be likely to contain calls made by the family members.

Applicants should not write about a potential or hypothetical 'error' and if the applicant can not identify any meaningful collateral intrusion that factor should be recorded in the application i.e. "none identified".

13) TIMESCALE **Identify and explain the timescale within which the data is required**	

GUIDANCE

TIME SCALE - Completion of this section assists the SPoC to prioritise the request.

DCG has an agreed Grading System that indicates to the CSP any urgent timescales, which is synchronised with the Urgent Oral Process (see footnote 40 and paragraph 3.56 of the code).

14) APPLICANT I undertake to inform the SPoC of any change in circumstances that no longer justifies the acquisition of the data			
Applicant's Signature		**Date**	

GUIDANCE

If the application is being recorded within a database (or other electronic format), and is attributable to the applicant, a signature is not required.

Considerations of the SPoC

An application, comments by the single point of contact (SPoC), considerations of the designated person, authorisations and notices may be made in writing ("paper") or electronically ("database").

15) ASSESSMENT BY ACCREDITED SPoC.	
How much will the acquisition of the data cost?	
Are there other factors the DP should be aware of? *For example, the requirement:* • *is NOT reasonably practical for the CSP to do;* • *will cause an adverse cost or resource implication to either your public authority or the CSP (for instance does the investigation or operation have the analytical capacity to undertake analysis of the communications data once acquired);* • *will produce excess data to that required.*	
Name of Accredited SPoC	

16) AUTHORISATION (Completed by Accredited SPoC when appropriate)	
Specify the reason why the collection of communications data by means of an authorisation is appropriate: ☐ There is an agreement in place between the public authority and the CSP relating to the appropriate mechanisms for the disclosure of the data ◇ ☐ The designated person considers there is a requirement to identify to whom a service is provided (for example subscriber check) but a CSP has yet to be conclusively determined as the holder of the communications data ♦ ☐ CSP is not capable of obtaining or disclosing the communications data Δ	
Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought.* Describe the course of conduct required to obtain the data.	☐ ◇Traffic or Service Use data – acquisition by SPoC directly from CSP ☐ ♦ Subscriber Information – acquisition by SPoC or, where SPoC can not acquire data directly from CSP, serve assurance of the Authorisation on CSP[1] ☐ ΔOther conduct – specify
The statutory purpose for which the conduct may be authorised is set out at section 8 of this form. *The office, rank or position of the designated person should be recorded within section 17 of this form together with a record of the date & time the granting of an authorisation is made.*	

*The question, *"Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought",* is appropriate where

[1] See paragraph 3.30 of the code

the communications data sought by the applicant may need refinement by the SPoC, for example incoming calls to a telephone number held by a CSP that does not keep a data set that can reveal such calls. The SPoC would state that several Authorisations and Notices will need to be undertaken with CSPs that can reveal calls instigating from their networks to the telephone number in question.

The designated person, having considered the comments of the SPoC, may decide the acquisition is not justified because of the significant resources required by the CSP to retrieve and disclose the data or it will be impractical for the public authority to undertake an analysis of the data.

It will also be appropriate for the SPoC to comment where the data sought by the applicant will require the acquisition of excess data, specifically where it is not practicable for the CSP to edit or filter the data, for example a specific incoming call in a data set with outgoing calls and cell site contained in it. If the designated person considers this to be necessary and proportionate for the acquisition of the specific incoming call then the Authorisation or Notice must specifically include the acquisition of the outgoing call, incoming calls and cell site.

Considerations of the Designated Person

An application, comments by the single point of contact (SPoC), considerations of the designated person, authorisations and notices may be made in writing ("paper") or electronically ("database").

17. DESIGNATED PERSON			
The designated person considers the application and if approved records their considerations: • *Why do you **believe** acquiring the communications data is necessary for one of the purposes within section 22(2) of the Act;* • *Why do you **believe** the conduct involved in obtaining the data is proportionate to the objective(s)? In making that judgement you should take in consideration any additional information from the SPoC. If the applicant has identified any meaningful degree of collateral intrusion, why you **believe** the request remains justified and proportionate to the objective(s)?*			
My considerations in approving / not approving this application are:			
This text box can be made bigger or smaller, it is not set out to indicate how much should be written			
☐ I authorise the conduct to be undertaken by the SPoC as set out in section 16 of this form. ☐ I give Notice and require the SPoC to serve it on (insert name of CSP) . The Notice* bears the unique reference number			
Name		Office, Rank or Position	
Signature		**Time and Date**	

GUIDANCE

The **DESIGNATED PERSON** must be able to show he or she has understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny.

The designated person should tailor their comments to a specific application as this best demonstrates the application has been properly considered.

If the designated person having read the application considers the applicant has met all the requirements then he or she should simply record that fact. In such cases a simple note by the designated person should be recorded.

There may be circumstances where the designated person having read the case set out by the applicant and the considerations of the SPoC will want to comment why it is still necessary and proportionate to obtain the data despite excessive data being acquired.

If the designated person does not consider the case for obtaining the data has been met the application should be rejected and referred back to the SPoC and the applicant.

*A Notice must include a unique reference number that also identifies the public authority. This can be a code or an abbreviation. For police services it will be appropriate to use the Police National Computer (PNC) force coding. See also paragraph 3.37 (and footnote 53) of the code.

If the designated person is recording their considerations within a database (or other electronic format) and is attributable to the designated person, a signature is not required.