NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS

Communications Data - Justifications and Priorities (Official Guidance)

Communications Data - Guidance on Justifications and Priorities

Policy Lead: _MI5 Warrantry Official_
Business sponsor: _Senior MI5 Official_
Policy Issue Date: November 2013
Review Date: November 2014

Policy Aim
To Provide applicants for Communications Data with the necessary information to draft justifications which effectively address both necessity and proportionality issues and to correctly assign National Priority Grading System (NPGS) grades to applications, as well as information for Designated Persons (DPs) to enable them to identify justifications that are incomplete or where NPGS priority grades have been inappropriately assigned.

Audience
All users of communications data.

Principles
- To provide simple and effective guidance to applicants for communications data on how to word justifications in requests for communications data
- To ensure the production of legally compliant justifications through the provision of comprehensive guidance
- To provide simple and effective guidance to applicants for communications data on how NPGS priority grades should be applied to applications
- To provide guidance for DPs on what information a proper justification should include and how to identify when an inappropriate NPGS priority grade has been assigned to an application

Summary

This page provides a resource for applicants and DPs for communications data, either using _**the electronic system for processing CD requests**_ or through the use of _**the relevant form**_. It outlines the issues of necessity and proportionality and how both should be addressed when justifying any applications for communications data. It also details how and when the different NPGS priority grades should be assigned. It should be noted however that _**the warrantry team**_ can advise only on legal compliance issues relating to communications data requests. Enquiries on how to make applications or to track the progress of existing applications should be directed to _**the relevant team.**_ [REDACTION]

Table of Contents

Justifications Overview

Core things to consider in any request for communications data are necessity, proportionality and collateral intrusion. Necessity, Proportionality and Collateral Intrusion require justification in their own separate boxes.

Necessity

Necessity can be divided into three main points that need to be considered in any communications data justification:

- A short background to the investigation - what is it that we are investigating?
- What role does the target that is associated with this request play in the investigation?
- How does the communications address that is the subject of this request relate to the target and to the investigation?

The applicant must be able to link these three points together in order to demonstrate that any request for communications data is necessary for the statutory purpose specified.

Proportionality – General

When considering proportionality, applicants need to outline how obtaining the data will benefit the investigation and what intrusion into privacy the request will result in. The main things that need to be considered are:

- What are you looking for in the data to be acquired?
- If the data contains what you are looking for, how will this assist you in taking the investigation forward?
- What will be the intrusion into the privacy of the target of the request? Will there be any other intended intrusion taking place?
- Is there another, less intrusive way of obtaining the information you need?
- If a time period of data has been specified, why is this particular time period required e.g. why would a shorter time period not be sufficient?

Therefore, the applicant should explain how the communications data will be used once obtained and how this will benefit the investigation. It is also important that intrusion into the target of the request's privacy is considered. These points form a large part of the proportionality argument, the other part being in relation to collateral intrusion.

Proportionality - Collateral Intrusion

Identifying any meaningful collateral intrusion forms part of the proportionality argument. The key question to be asked in relation to this 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?
- If a time period of data has been specified, how will this impact on the identified collateral intrusion?
- How do you plan to manage any identified collateral intrusion? [REDACTION]

"Meaningful collateral intrusion" includes collateral intrusion that we can foresee is "highly likely" – such as family members using the landline or internet connection where they live. However, we should not speculate where possible collateral intrusion cannot be said to be "highly likely". So when considering this question, the applicant should not detail potential or hypothetical errors. [REDACTION]
Therefore, collateral intrusion should always be considered and described if it is identified. However, it may be that none can be identified. When this is the case, then this should be stated. For example, telephone subscriber checks are unlikely to result in any collateral intrusion.

Priorities Overview

Requests for communications data are graded on a nationally agreed, three point scale before being sent to the relevant Communications Service Provider (CSP). This process, which is detailed in the Communications Data code of practice, is called the National Priority Grading System (NPGS). It ensures that CSPs are able to manage their workload effectively and ensure that the most urgent requests are dealt with first.

NPGS Priority Grades Explained

Requests for communications data can be assigned one of three NPGS priority grades, the definitions of which are provided below:

1 – Very Urgent. [REDACTION]
2 – Urgent. [REDACTION]
3 – Routine. The majority of applications will fall into this category
[REDACTION]

Guidance for Designated Persons

Designated Persons (DPs) are responsible for granting authorisation for communications data requests. They must ensure that the request is both necessary and proportionate for the purpose for which the data is sought. DPs should take care to scrutinise the application, particularly the justification page, before authorising any request for communications data. In particular, key points DPs should check are:

- Taking into account the guidance for applicants above, that the justification provided by the applicant is sufficient to satisfy the DP that obtaining the requested data is both necessary and proportionate
- That the individual mentioned in the justification is identical with the one for which the data is being obtained, that is that the justification has not been "copied and pasted" from another application
- That the intrusion into privacy that will result from the request has been addressed where necessary and where identified, measures to mitigate collateral intrusion have been outlined. In relation to subscriber details it is accepted that collateral intrusion is likely to be minimal or that none will be identified
- That the time period of data requested is proportionate and that the reasoning for requesting the time period listed is explained in the justification DPs are required to reject any application for communications

data where they are not convinced of both the necessity and proportionality of the request. DPs are encourage to consider carefully whether necessity and proportionality have been appropriately considered. When rejecting applications, DPs should comment on their reasons for rejection in the appropriate box on *__the electronic system for processing CD requests__* of communications data or on the *__relevant form__* that is submitted.

In relation to NPGS grades, DPs should check that they agree with the urgency grade that the applicant has set for an application and if they agree, they may wish to comment on this, although it is not compulsory to do so. If DPs do not agree with the priority grading the applicant has chosen then they can downgrade or upgrade the priority as applicable. Where a DP has changed the priority they must justify the reasons for the change in the "DP justification" box in the "priority" page.

DPs are also encouraged to familiarise themselves with both the Communications Data code of practice and the Data Communications Group (DCG) justifications guidance. Both of these documents are available via the links to the right of this page.

ANNEX A

Example *__the Electronic System for Processing CD Requests__* Justifications

Listed below are a few examples of justifications for some of the most common *__the electronic system for processing CD requests__* requests:

[REDACTION]

ANNEX B

Scenarios for NPGS Grades 1 and 2
Scenarios are provided below giving example of when NPGS grades 1 or 2 could be applied:

[REDACTION]

ANNEX C

Examples for Communications Related Data intrusion issues

[REDACTION]