



**HEDDLU
DYFED-POWYS
POLICE**

ACCESSING COMMUNICATIONS DATA

FORCE POLICY

Author:	DC Cerys Pickard
Version:	0.01
Date:	April 2008
Person Responsible:	DCC Edwards

POLICY IDENTIFICATION PAGE

THIS POLICY HAS BEEN DRAFTED IN ACCORDANCE WITH THE PRINCIPLES OF HUMAN RIGHTS LEGISLATION, PUBLIC DISCLOSURE IS APPROVED UNLESS WHERE OTHERWISE INDICATED AND JUSTIFIED

POLICY TITLE: Accessing Communications Data Force Policy

POLICY REF. NO: XX / 08

POLICY OWNERSHIP: Dyfed-Powys Police

PORTFOLIO/BUSINESS AREA OWNERSHIP: CM&RD

DEPARTMENT RESPONSIBLE: CM&RD

PERSON RESPONSIBLE: Detective Chief Superintendent

LINKS/OVERLAPS WITH OTHER POLICIES:

POLICY IMPLEMENTATION DATE: 18th June, 2008

REQUIRED FREQUENCY OF REVIEW: Annually

DATE POLICY LAST REVIEWED: New Policy Document

POLICY REVIEW DATE: 1st June, 2009

CERTIFICATE OF COMPLIANCE

This policy has been drafted in accordance with the Human Rights Act and has been reviewed on the basis of its contents and the supporting evidence and it is deemed compliant with that Act and the principles underpinning it.

Name: Samantha Gainard

Department: Legal Services Department

Samantha Gainard

Signed: (Force Legal Advisor)

REVIEW

June, 2009

This policy is due for review by:

Review of Document

Date of Review	Reviewed by:	Amendments made

Contents

<i>Section</i>	<i>Page</i>
General Principles	6
Aim and Lawful Authority	6
Definition of Communications Data	7
Contact with UK's Communication Industry	7
Role of Covert Operations Registry	7
Types of Communications Data that can be requested.	7
Nuisance Calls	9
Application Process & Justification	9
Levels of Authority	10
Out of Hours Requests	10
National Prioritisation Grades	10
Disclosure of Data in Evidence	11
Application Process Overview	12

Policy Document Statement

This Policy has been drafted in accordance with the Human Rights Act 1998

General Principles

It is the policy of Dyfed-Powys Police:

- To deliver guidance in respect of the management and procedures in relation to accessing communications data.
- To clearly define administrative duties in support of key policing objectives.
- To provide key information to front line officers.
- To work in partnership with other agencies to protect the public and prevent crime.

All staff, in the adoption of this policy, and in the exercise of their daily duties, must ensure that:

- a. They follow a clearly defined decision making process by detailing their objective(s), assessing all available and relevant information and feasible options, documenting decisions, and reviewing outcomes;
- b. They give due regard to the welfare, safety, general well being and human rights of all individuals;
- c. They do not unjustifiably discriminate against any individual or groups of individuals;
- d. Actions taken are justified, strictly proportional to, and are the less intrusive and damaging option to the achievement of their legitimate aims;

Aim and Lawful Authority

The purpose of this policy is to provide guidance to police personnel on the accessing communications data within the Force.

The legal basis for the exercise of powers and duties outlined in this policy are:

- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000

Dyfed-Powys Police consider that these actions are necessary in a democratic society in the interest of, and in order to safeguard:

- Public safety
- The prevention of disorder or crime
- The protection of public order
- The protection of rights and freedoms of others

1. Definition of communications data

The acquisition of ‘communications data’ is provided by Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 (RIPA 2000).

The term ‘communications data’ embraces the ‘who’, ‘when’, and ‘where’ of a communication. What it does not include is the content of what was said or written during the communication. In essence this relates to data held in respect of telephone, internet or postal communications.

2. Contact with UK’s Communication Industry

The Force Covert Operations Registry based at Force Headquarters within CM&RD have primary responsibility to communicate with the Police Liaison Units within the various companies making up the UK’s communication industry. Within normal working hours only accredited SPOC Officers within this department can communicate directly with these companies. Out of hours requests can be dealt with via the Force Communications Centre. The procedure for this is detailed in Section 8 of this document.

3. Role of Covert Operations Registry

Accredited SPOC Officers within the Covert Operations Registry have responsibility for the following: -

- Initial vetting and scrutiny of all applications to ensure that the acquisition of the material sought is lawful, necessary, justified and proportionate to the offences under investigation.
- Receiving “raw” data material from the Communications service providers and producing them to the Investigating Officer.
- Advising on Authority levels and disclosure issues in relation to all communications data (including data provided for intelligence purposes only)
- Creating an administrative environment that is secure and able to withstand a detailed audit by external commissioners appointed to oversee the process.
- Providing a 24-hour call out cover to enable access to communications data out of hours (where the necessary criteria are met) and to assist with urgent RIPA authorities.

4. Types of Communications Data that can be requested.

Communications data is divided into three categories: Account Information, Service Use Information, and Traffic Information. These are explained below.

Account Information

This is more widely known as subscriber information and relates to information that may be held by the service provider about the person who holds a specific account with them.

Some examples of information that can be obtained:

- Who is the subscriber of telephone number 01234 567890?
- Who pays the accounts for telephone number 01234 567890?
- What are the top-up details of telephone number 01234 567890?
- Who is the account holder of e-mail account xyz@xyz.anyone.co.uk?

This type of information can be used in evidence.

Service Use Information

Examples of information that can be obtained is as follows:

- Itemised records of connections to internet services, i.e. IP Log in history from an e-mail address. This can tell us what computers the person using the e-mail has logged on to during a specified period.
- Itemised records of outgoing calls made by mobile or landline telephones. This includes times of calls and durations.
- IMEI traces – this can establish what SIM cards have been placed in the IMEI (Handset) during a specified period.
- Mail re-direction – Royal mail can inform the relevant Law Authority if there are existing re-direction instructions on a specified address during a specified period.

This type of data can be used in evidence.

Traffic Information

This is data that the user/owner of a telephone or computer normally has no control over.

Examples of what can be obtained is as follows:

- Live Cellsite – This is the live monitoring of a mobile phone when it is switched on and provides most details of the location.
- Historic Cellsite – This is an historic picture of the above, i.e. where the mobile phone was at a specified date and time.
- Incoming billing – This is a list of calls made to the mobile phone
- Mail Monitoring – Royal mail can list the letters/packages delivered to a specified address during a specified time. This information cannot be obtained

historically as advance measures are set up prior to the information being obtained.

Data received under this category is initially supplied 'FOR INTELLIGENCE PURPOSES ONLY'. Should there be a requirement to disclose live cellsite in a suspect interview or subsequently use as evidence, then this will require the prior consent of ACPO. This can be obtained by the submission of a report to the Covert Operations Registry outlining why the data is deemed critical to the prosecution.

5. Nuisance Calls

This can relate to the most minor of calls, which includes a silent line, to the most serious of threats made to the user of a telephone.

When such reports are made and an investigation is commenced, the victim should be advised to contact the service provider in the first instance so that the calls can be monitored by them and they can subsequently provide the police with this information free of charge. The victim should also be encouraged to keep a note of the time/date and content of all such calls

Should these calls be persistent, or there is a need, then the tape recording of these calls should be considered as an investigative option to provide the best evidence. This can be done with the consent of the victim and with a Directed Surveillance application following which the Force Technical Support Unit can set-up the equipment.

6. Application Process and Justification

All applications and authorisations will be documented on Charter/Swallow unless grounds of urgency can be justified.

All applications must be documented so as to satisfy the requirements of RIPA 2000. To meet these requirements, applicants must show that the application is both necessary and proportional. It should also consider issues surrounding collateral intrusion and detail how this will be minimised.

Necessary – Why is it necessary to the enquiry to obtain this data? What is sought to be achieved from so obtaining it? Why has the date and time period been requested?

Proportional – How will the data achieved the objectives of the enquiry? Why can't the objectives be achieved by any less intrusive means?

Collateral Intrusion – Is intrusion into the privacy of innocent third parties. It is important to detail any plans to minimise collateral intrusion.

7. Levels of Authority

Authority levels of the required information is listed below:

- Account Information - Inspector or above.
- Service Use Information - Superintendent or above.
- Traffic Data - Superintendent or above.

8. Out of Hours Requests

All urgent requests for telecommunications data out of hours must be referred to the duty Inspector within the Force Communication Centre. To facilitate this process it is the responsibility of the duty inspector to contact the 'on call' SPOC.

Once contacted, the SPOC should be provided with the STORM reference number, the nature of the enquiry and the contact details of the 'on call' or duty Superintendent. In cases of urgent subscriber checks, these can be authorised by the Operations Room Inspector.

It is the responsibility of the SPOC to collate all the information subject of the request and authorisation.

In relation to dropped 999/112 calls, there exists a "golden hour" which is the hour following the initial receipt of such a call. Within this period the Operations Room may approach the relevant service provider for subscriber information without recourse to the RIPA legislation. This is on the basis of such calls emanating from somebody who is in immediate need of emergency assistance whereby issues of danger and harm exist. The Operations Room Inspector has the responsibility of collating such calls.

9. National Prioritisation Grades

Upon receipt of an application within the Covert Operations Registry it is the responsibility of the SPOC to grade the request using the National Standard of Prioritisation. The grades are as follows:

Grade 1

An immediate threat to life such that a person's life might be endangered if a communications service provider who had been given notice (written or oral), did not undertake a course of action for the acquisition and disclosure of communications data that was practicable for the CSP to undertake, and it was not practicable for the SPoC to undertake the acquisition of the data by means of an authorisation (where an on-line service is provided by the CSP)

Grade 2

There is a general undertaking by CSPs that when served with a notice (written or oral) they will respond promptly within their normal office hours and the CSP may on a case by case basis and in consultation with the SPoC make arrangements during office hours for an out of office hours response where it is confirmed there is;

- An exceptionally urgent operational requirement where, within no more than 48 hours of the notice (written or oral) being given, the acquisition of communications data will directly assist the prevention or detection of the commission of a serious crime (*note serious crime is as defined by See Section 81(2) of RIPA*) and the making of arrests or the seizure of illicit material, and where that operation opportunity will be lost if a communications service provider who had been given notice (written or oral), did not undertake a course of action for the acquisition and disclosure of communications data that was practicable for the CSP to undertake, and it was not possible for the SPoC to undertake the acquisition of the data by means of an authorisation (where an on-line service is provided by the CSP); or
- A credible and immediate threat to national security or a time-critical and unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost, if a communications service provider who had been given notice (written or oral), did not undertake a course of action for the acquisition and disclosure of communications data that was practicable for the CSP to undertake, and it was not possible for the SPoC to undertake the acquisition of the data by means of an authorisation (where an on-line service is provided by the CSP).

Grade 3

All other notices for the acquisition and disclosure of communications data. The SPOC should indicate any specific or critical time issues, which will impact upon the investigation or operation if necessary.

10. Disclosure of Data in Evidence

Requests for statements from the telecommunications industry must be made via the SPoC. Every effort must be made to serve the telecommunication evidence voluntarily or by virtue of Section 10 Criminal Justice Act 1967.

As previously stated within this document Live cellsite analysis and Cell dumps are strictly FOR INTELLIGENCE PURPOSES ONLY and must not be disclosed unless with the authority of ACPO.

11. Application Process Overview

A flow chart is attached at '*Appendix A*' that outlines to application process.

Appendix 'A'

Application Process – Flow Chart

