RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

CABINET

25TH FEBRUARY 2021

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) - USE OF RIPA IN 2019-2020 BY RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL AND THE COUNCIL'S CORPORATE ENFORCEMENT POLICY

REPORT OF THE DIRECTOR OF LEGAL SERVICES IN DISCUSSIONS WITH THE DEPUTY LEADER, CLLR WEBBER

Authors: Judith Parry, Trading Standards & Registrar Service Manager
Andy Wilkins, Director of Legal Services

1. PURPOSE

To enable Members to review:

1.1 The Council's use of the Regulation of Investigatory Powers Act 2000 (as amended) (RIPA) for the period 1st April 2019 to 31st December 2020, including the Investigatory Powers Commissioner's Office (IPCO) audit response; and

1.2 The new Corporate Policy and Procedures Document on the Acquisition of Communications Data under the Investigatory Powers Act 2016 (IPA).

2. RECOMMENDATIONS

It is recommended that Cabinet:

2.1 Notes the contents of this report;

2.2 Acknowledges RIPA has been used in an appropriate manner that is consistent with the Council's RIPA policies during the period 1st April 2019 – 31st December 2020;

2.3 Approves the updated Corporate Policy and Procedures Document on the Acquisition of Communications Data under the Investigatory Powers Act 2016 (IPA) attached as Appendix B to the report; and

2.4 Approves a change of reporting period to a calendar year, to align with the changed IPCO returns period.

3. REASONS FOR RECOMMENDATIONS

3.1 To ensure Members are kept appraised of how RIPA has been used during the period 1st April 2019 - 31st December 2020 and that it has been used in an appropriate manner consistent with the Council's RIPA policies.

3.2 The Cabinet is responsible for approving revisions to the Council's Corporate Enforcement Policy and Corporate RIPA and IPA Policies in order to ensure that they remain fit for purpose.

4. USE OF RIPA BY THE COUNCIL: 1ST APRIL 2019 – 31ST DECEMBER 2020

Directed Surveillance and the use of Covert Human Intelligence Sources

New Authorisations

4.1 During the period 1st April 2019 - 31st December 2020, there were four authorisations in respect of directed surveillance. During the same period, there were no authorisations for the use of covert human intelligence sources.

4.2 Directed surveillance authorisations can be issued where it is necessary and proportionate in order to prevent or detect crime, or prevent disorder, where at least one of the offences is punishable by a maximum term of imprisonment of at least six months or more or relates to the underage sale of alcohol or tobacco/nicotine.

4.3 All four directed surveillance authorisations related to fly tipping.

Authorisations extant as at 1st April 2019

4.4 There were no authorisations in respect of directed surveillance that had been authorised in the previous financial year (2018-19) and were carried forward. Similarly, no authorisations in respect of a Covert Human Intelligence Source extant remain extant.

Cancellation of Authorisations & Subsequent Outcomes

4.5 All four authorisations were reviewed and extended at the statutory 12-week period, and then cancelled a month further into the second 12-week period.

4.6 The outcomes of the surveillance operations that were concluded were as follows:

Evidence of fly tipping at location under investigation

- 1 x authorisation identified fly tipping which included an oil drum containing unknown substances; this matter is currently being taken forward as a joint investigation with Natural Resources Wales
- 1 x authorisation identified various instances of fly tipping; these matters are currently being investigated
- 1 x authorisation identified fly tipping, but neither a registration number nor image of offender was able to be obtained from the recording

<u>No evidence of fly tipping at location identified</u>

- 1 x authorisation resulted in no instance of fly tipping, but disposal of litter observed; this matter is currently being investigated

Authorisations extant as at 1st January 2021

4.7 No investigations have been carried over into 2021.

4.8 The outcomes demonstrate how the use of directed surveillance is able to produce results that are of benefit from an enforcement point of view. Without the use of directed surveillance, officers would not have been able to progress the investigation to determine whether the alleged incidents were ongoing: directed surveillance has therefore enabled officers to ascertain the true situation at the relevant locations, in a manner that was the most cost-effective in relation to officer time.

Human Rights Act Authorisations

4.9 As part of initial investigations, officers may need to carry out non-overt work which does not fall within the statutory requirements for RIPA, mainly because the work is carried out in such a manner that there is little likelihood of obtaining private information (collateral intrusion). The use of non-overt enforcement techniques are assessed to ensure that they are carried out in compliance with the requirements of the Human Rights Act 1998 (HRA). Such assessments are recorded on a Human Rights Act consideration form, whereby the necessity, proportionality and purpose of the activity are addressed, precautions are introduced to minimise collateral intrusion and the use of the technique is approved by a senior manager.

4.10 Importantly, if the initial work carried out using the HRA-compliant technique shows that an investigation needs to be carried out using RIPA-based techniques, officers will apply for RIPA authorisation.

4.11 During the period of this report, the HRA authorisations were:

	1st April 2019 – 31st March 2020 (12 month period)	1st April 2020 – 31st December 2020 (9 month period)
Anti-social behaviour monitoring	0	0
Underage sales test purchasing	0	0
Proxy sales monitoring	0	0
Internet site monitoring	25	81
Vehicle test purchasing	0	0

4.12 Of note this period is the increase in internet site monitoring. Such sites are predominantly monitored for investigations into sale of illegal product via social media; it can be seen from the table that during the 2019-20 financial year, this amounted to 25 complaints and investigations. Since April 2020, the number stands at 89 for a 9-month period. Internet site monitoring has been carried out for diverse means during the coronavirus pandemic, including:

- Investigation into potential PPE suppliers to ensure that the product supplied are legally compliant and safe;
- Investigation of 'events' advertised during periods when these were prohibited by the Health Protection (Coronavirus Restrictions) (Wales) Regulations
- Determination of whether premises required to be closed during coronavirus restrictions were still trading in breach of the Regulations
- Review and assessment of legal compliance in relation to businesses which are new (e.g. manufacture and sale of 'bath bombs'), or who have deviated from usual trading practice (e.g. restaurants who were unable to open, moving to home delivery services)
- A means of contacting traders to provide proactive advice during pandemic legislative changes; close contact services, such as hairdressers and beauty therapists commonly have social media profiles, and this is a trade sector which has been subject to many changes throughout the pandemic

4.13 A review of these operations and investigations showed that on no occasion did they result in an improper infringement of a person's human rights.

Communications Data

4.14 During the reporting period, eight applications for communications data were submitted via the National Anti-Fraud Network (NAFN) in relation to telephone numbers used as part of fraudulent activity.

5 AUDIT BY THE INVESTIGATORY POWERS COMMISSIONER'S OFFICE (IPCO)

5.1 On 7th September 2020, the IPCO conducted a 3-yearly audit on the appropriate use of RIPA within Rhondda Cynon Taf. In previous years this has been a physical visit, but due to coronavirus restrictions, this audit was carried out remotely.

5.2 Prior to the audit date, information and authorisations were sent to the auditor, Mr Paul Gration; during the audit itself, Mr Gration asked about processes and policies, and also provided some recommendations in respect of refresher training in the use of RIPA. Training is scheduled to take place every 3 years, but this year was suspended due to the pandemic and the Council response to it.

5.3 The audit report was received on 14th September 2020 from the Rt. Hon. Sir Brian Leveson, Investigatory Powers Commissioner, who was complementary of both the RIPA use and procedures in place within the local authority. A copy of the full response is appended at Appendix A to the report.

5.4 It is likely that future audits will be carried out remotely, based both on the amount of RIPA activity within Rhondda Cynon Taf and its overall compliance.

6 THE CORPORATE POLICY AND PROCEDURES DOCUMENT ON THE ACQUISITION OF COMMUNICATIONS DATA UNDER THE INVESTIGATORY POWERS ACT 2016 (IPA)

6.1 The commencement of the Investigatory Powers Act on 11th June 2019 meant that information requested in relation to communications data, is now provided electronically and submitted to the Office for Communications Data Authorisations (OCDA) via the National Anti-Fraud Network (NAFN).

6.2 Previously, requests for authorisation were required to be submitted to the Magistrate Court. The new process provides standardisation in format. NAFN ensure the request is proportionate, justified and meets the requirements of the IPA; the OCDA authorise approvals, and NAFN approach the Communications Services Provider(s) to obtain the requested data on behalf of the Local Authority.

6.3 The introduction of the new Act and process has resulted in the drafting of a new Corporate Policy for the Acquisition of Communications Data which is attached as Appendix B to the report.

7. REPORTING PERIOD GOING FORWARD

The IPCO has amended their annual return period to be a calendar year; it is suggested that the report on the Council use of RIPA is similarly amended to align to the calendar year.

8. CONSULTATION

This report has been prepared in consultation with the Council's Trading Standards & Registrar Service Manager who is responsible for operational oversight of RIPA matters.

9. EQUALITY AND DIVERSITY

There are no equality or diversity implications linked to this report.

10. FINANCIAL IMPLICATIONS

There are no financial implications linked to the contents of this report.

11. LINKS TO THE COUNCIL'S CORPORATE PLAN/ OTHER COUNCIL PRIORTIES

The report will ensure that effective governance arrangements with regards to RIPA remain in place by the Council.

12. CONCLUSION

The Senior Responsible Officer (Director of Legal Services) considers that RIPA has been used appropriately in relation to all of the above uses of directed surveillance and acquiring of communications data and that RIPA has been used in a manner that is consistent with the Corporate policies.

IPCO
Investigatory Powers Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Christopher Bradshaw
Chief Executive
Rhondda Cynon Taf County Borough Council
The Pavilions
Cambrian Park
Clydach Vale
Tonypandy
CF40 2XX

chiefexecutive@rctcbc.gov.uk

14 September 2020

Dear Mr. Bradshaw,

Inspection of Rhondda Cynon Taf County Borough Council

Please be aware that IPCO is not a "public authority" for the purpose of the Freedom of Information Act (FOIA) and therefore falls outside the reach of the FOIA. It is appreciated that local authorities are subject to the FOIA and that they may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the attention of the IPCO Data Protection Officer (at: info@ipco.org.uk), before making any disclosure. This is also the case if you wish to make the content of this letter publicly available.

Your Council was recently the subject of a telephone-based inspection by one of my Inspectors, Mr Paul Gration. I am grateful to Andrew Wilkins, your Director of Legal Services and RIPA Senior Responsible Officer, who provided all the relevant information and supporting documentation and organised the call. He was joined on the call by Judith Parry, who has participated in previous inspections, and both provided helpful and relevant contributions.

The information provided has demonstrated a level of compliance that removes, for the present, the requirement for a physical inspection. I ask you to consider and to ensure that any observations from the findings of the remote inspection are promptly addressed.

The Council's previous inspection was conducted by Mr Neil Smart, who made a number of recommendations which have been discharged by Mr Gration, who has made some minor observations of his own. I understand, following receipt of my correspondence outlining my expectations regarding handling of data, that you are well placed with regard to the required safeguarding measures. Mr Gration was reassured your SRO has a strong understanding of the requirements, and a number of appropriate measures are in place which are supported by the relevant corporate policies.

It is good to hear that you are maximising your membership of the National Anti-Fraud Network (NAFN) and this process is supported by your recently updated corporate policy for the Acquisition of Communications Data.

As stated, Mr Gration has made some minor observations which require some attention. The finer details of these points, along with others, have been fully discussed with Mr Wilkins and Ms Parry. He has highlighted the Council's RIPA Policy and Procedure as a well written and regularly updated document which incorporates recent legislative changes. The policy however details a long list of Authorising Officers. Mr Gration has discussed, with Mr Wilkins, the benefits of reducing that list and developing a smaller number of confident and competent Authorising Officers.

His main observation relates to the level of knowledge of RIPA across the organisation. There is a clear need to refresh the training (last delivered in 2016) of those actively involved in this area of investigation, but also to increase the awareness across the wider organisation. This will help the organisation to continue to deliver a high level of compliance.

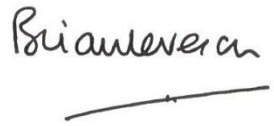
In conclusion, although your Council is a limited user of its surveillance powers, I take the opportunity here to reiterate to you the importance of regular, ongoing internal oversight of the actual or potential use of these powers, which should be managed through your Senior Responsible Officer.

It is also important that officers engaged in investigatory or enforcement areas where RIPA considerations are not so immediately apparent, maintain their levels of knowledge and know whom to approach for guidance. Mr Wilkins, as your SRO, has given the appropriate reassurance that the integrity of your Council's processes and governance procedures will be maintained to ensure that high standards of compliance with the Act and relevant codes of practice are achieved.

I hope that you find this letter to be helpful and constructive. My Office is available to you should you have any queries following the recent inspection, or at any point in the future. Contact details are provided at the foot of this letter.

I shall be grateful if you would acknowledge receipt of the report within two months.

Yours sincerely,



The Rt. Hon. Sir Brian Leveson
The Investigatory Powers Commissioner

RHONDDA CYNON TAF
COUNTY BOROUGH COUNCIL

CORPORATE POLICY & PROCEDURES DOCUMENT

ON

THE ACQUISITION OF COMMUNICATIONS DATA UNDER

INVESTIGATORY POWERS ACT 2016 (IPA)

Andrew Wilkins
Director of Legal and Democratic Services,
The Pavilions,
Cambrian Park,
Clydach Vale
Tonypandy

Adopted on 10th March 2008

Revised August 2008, December 2010, February 2013, September 2014, June 2015, November 2019, [December 2020 – Subject to Cabinet approval]

CONTENTS PAGE

Introduction and Key Messages

1. This Corporate Policy & Procedures Document is based upon the requirements of The Investigatory Powers Act 2016 ('IPA') and Home Office's Code of Practice on Communication Data. The Council takes responsibility for ensuring the IPA and RIPA procedures are continuously improved.

2. The authoritative position on IPA is, of course, the Act itself and the associated Home Office Codes of Practice and any Officer who is unsure about any aspect of this Document should contact, at the earliest possible opportunity, the Senior Responsible Officer for advice and assistance. Appropriate training and development will be organised by the Senior Responsible Officer to relevant Authorising Officers and other senior managers.

3. Copies of this Document will be placed on the Intranet.

4. The Senior Responsible Officer has authorised the Council's Lead Officer for IPA and Accessing Communications Data to maintain the Corporate Register of all IPA communications data requests, but this register will be subject to examination by the Senior Responsible Officer as and when it is deemed necessary. All forms completed in respect of Communications Data are requested and maintained electronically on the National Anti-Fraud Network (NAFN)

5. IPA and this Document are important for the effective and efficient operation of the Council's actions with regard to acquiring communications data. This Document will be kept under review by the Senior Responsible Officer. Authorising Officers must bring any suggestions for continuous improvement of this Document to the attention of the Senior Responsible Officer at the earliest possible opportunity.

6. If you are in any doubt on IPA, this Document or the related legislative provisions, please consult the Senior Responsible Officer, at the earliest possible opportunity.

Effective Date of Operation and Authorising Officer Responsibilities

1. The Corporate Policy and Procedures provided in this Document became operative with effect from the date of its adoption by the Council, that is 10th March 2008. The commencement of the IPA on 11th June 2019 means that information is provided electronically and submitted to the Office for Communications Data Authorisations (OCDA) via NAFN, which provides standardisation in format. It is essential that Chief Officers and Authorising Officers in their Divisions take personal responsibility for the effective and efficient operation of this Document.

2. Chief Officers have designated Authorising Officers within the appropriate divisions to take action under RIPA. These persons are detailed in the Corporate Policy and Procedures Document on Regulation of Investigatory Powers Act and as Authorising Officers they are entitled to act as Designated Persons for acquiring communications data.

3. Authorising Officers will also ensure that staff who report to them follow this Corporate Policy & Procedures Document and do not undertake or carry out any obtaining of communications data without first obtaining the relevant authorisations in compliance with this Document.

ACQUISITION OF COMMUNICATIONS DATA

Introduction

The Investigatory Powers Act 2016 controls the acquiring of communications data by public authorities; Section 73 of states that a Local Authority is a public authority for the purposes of acquiring specific communications data. Communications data does not include the content of the communications such as the e-mail message, the letter or text, or the content of the phone call.

Part 3 of the IPA introduces a statutory framework to regulate access to communications data by public authorities consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in these processes, and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights (ECHR), in order to balance the rights of the individual against the needs of society as a whole to be protected from crime and other public safety risks.

The acquisition of communications data under the Act will be a justifiable interference with an individual's human rights under Article 8 of the ECHR only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with the law.

As a result officers should not require, or invite, any postal or telecommunications operator to disclose communications data either by using other statutory powers or by exercising any exemption to the principle of non-disclosure under the Data Protection Act 1998. Such a statutory power may only be used if the power explicitly provides for the obtaining of communications data.

The Office for Communications Data Authorisations

The Office for Communications Data Authorisations (OCDA) is the first organization of its kind in the world and commenced its operations in March 2019. The OCDA assesses Communications Data applications from public authorities and makes decisions about those applications to ensure a fine balance between protection of privacy and risk to public safety.

Under the IPA, OCDA will be responsible for ensuring that any applications made by relevant authorities in the UK are assessed independently, rigorously and in line with the newly strengthened legislation. OCDA will act as a hub of authorization expertise, independently assessing applications, holding authorities accountable to robust safeguarding standards, and challenging where required.

Local Authorities must submit all their communication data applications via NAFN for the consideration of the OCDA. All applications must be authorised by OCDA prior to any communications data being acquired on behalf of a Local Authority.

What is Communications Data and what categories are there

Communication data is information about communications: the "who, when, where and how" of a communication but not the content: what was said or written. It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning of the communication. It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or e-mail address of the originator and recipient, unanswered call attempts and the location from which the communication was made. It covers

electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

An operator who provides a postal or telecommunications service is described as a Communications Service Provider (CSP).

IPA defines telecommunications data in two categories:

a) **Entity Data**
Is about an entity (person), an association between, or part of, a telecommunications service and an entity. It includes data that identifies or describes the entity.

b) **Events Data**
Identifies or describes an event, whether or not be reference to its location, on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.

Communications Data that can be acquired

A Local Authority can acquire entity and events data. Examples are provided below:

Entity Data (IPA s261(3))

- 'Subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- Subscribers' or account holders' information, including names and addresses for installation, and billing payment method(s), details of payments;
- Information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;
- Information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes (which includes Personal Unlocking Key codes for mobile phones); and
- Information about selection of preferential numbers or discount calls.

Event Data (IPA s261(4))

- Information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- Information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- Information identifying the sender or recipient (including copy receipts) of a communication from data comprised in or attached to the communication;
- Routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- Itemised telephone call records (numbers called);

- Itemised internet connection records;
- Itemised timing and duration of service usage (calls and/or connections);
- Information about amounts of data downloaded and/or uploaded; and
- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

NB Local Authority staff are only permitted to acquire and disclose communications data for the purpose of preventing or detecting crime or of preventing disorder. This purpose should only be used in relation to the specific (and often specialist) offences or conduct that the Council has been given the statutory function to investigate. Events data can only be acquired if the offence being investigated meets at least one of the definitions of serious crime: this includes an offence that is capable of attracting a prison sentence of 12 months or more, or where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common goal.

In a joint investigation between the Council and another enforcement authority, such as the police, either authority may acquire any communications data under IPA to further the joint investigation where to do so is necessary and proportionate.

How to obtain Communications data

The annex to this document provides a simplified summary of the application process for communications data.

Acquiring communications data can only be carried out by means of the National Anti-Fraud Network (NAFN) secure website. To use this system Applicants have to register individually on the NAFN website at www.nafn.gov.uk. Once registered the Applicant completes the application form online and it is then submitted electronically to one of the SPOCs at NAFN. The accredited SPOCs at NAFN provide independent scrutiny of the applications, It is important that the Applicant consult with a NAFN SPOC throughout the authorisation process. The NAFN SPOC will advise the Applicant of any need for changes to the application form. After the SPOC considers the application satisfactory, the Designated Person will then receive an e-mail to say that there is an application form on the website for him or her to consider. The Designated Person completes the relevant part of the form to provide his or her decision. The NAFN SPOC then uses the authorisation process to obtain the required communications data from the CSP database and that data is posted on the website so that only the Applicant can access it. If NAFN do not have direct access to the database of the relevant CSP their SPOC will send a notice to the CSP in the usual way.

Applying for Communications data

The investigating officer will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring communications data. An application to acquire communications data must:

- Describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- Specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- Include a unique reference number;

- Include the name and the office, rank or position held by the person making the applications;
- Describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- Include the operation name (if applicable) to which the application relates;
- Identify and explain the time scale within which the data is required;
- Explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- Present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;
- Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and what that intrusion is justified in the circumstances;
- Consider and, where appropriate, describe any possible unintended consequences of the application; and
- Where data is being sought from a telecommunications operator or postal operator, specify whether they may inform the subject(s) of the fact that an application has been made for their data.

The time scale is based on set Priorities 1 to 4. Local Authorities may no select Priority 1; most Local Authority requests fall within Priority 4 'Routine' for which the service level expectation is within 4 working days (60 working hours).

It is good practice for the Applicant to state on the Application Form if they have carried out any open source checks on the telephone numbers or communications addresses that are under investigation; this assists with justifying the principle of proportionality

The Applicant may request historic data or future data, by which the Communications Service Provider must provide details of, e.g. all outgoing telephones or Internet connections over a set future period of up to a month. Requests for such future data are considered more intrusive than requests for historical data.

The form is then passed electronically to the appropriate NAFN accredited Single Point of Contact for Accessing Communications Data (SPOC).

Communications data should be treated as information with a classification of OFFICIAL and a caveat of SENSITIVE. The SENSITIVE caveat is for information that is subject to 'need to know' controls so that only authorised persons can have access to it. This does not preclude the lawful disclosure of material when required; it makes clear that the information must be treated with care and must also be stored and handled in accordance with the duties under the Data Protection Act.

Data Relating to Certain Professionals

Communications data is not subject to any form of professional privilege, since the fact that a communication has taken place does not disclose its contents. However the degree of interference with privacy may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or confidential information (such as a medical doctor, lawyer, journalist, MP, AM or minister of religion). It may also be possible to infer sensitivity from the fact that someone has regular contact with say a lawyer or journalist.

Such situations do not preclude an application being made. However, special consideration should be given to necessity and proportionality, drawing attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly privacy and where it might be engaged, freedom of expression. Applicants must clearly note when an application is being made for the communications data of such a professional. This will also need to be recorded on the Authority Central Record.

Issues surrounding the infringement of the right to freedom of expression may arise when a request is made for the communications data of a journalist. There is a strong public interest in the willingness of sources to provide information to journalists anonymously. If an application is intended to determine the source of journalistic information, there must be an overriding requirement for it to be in the public interest. Even if it is not intended to determine the source of journalistic information there is still a risk of collateral intrusion into legitimate journalistic sources, so particular care should be taken to properly consider the public interest in whether the intrusion is justified. This should include drawing attention to whether alternative evidence exists or whether there are alternative means to obtain the information. Identification of journalist sources can only be sought by using production orders under PACE, which are not available to the council. Judicial oversight does not apply where applications are made for the communications data of those known to be journalists, but where the application is not to determine the source of journalistic information, for example where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation.

Communications data that may be considered to determine journalistic sources includes data relating to:

- Journalists' communications addresses;
- Communications addresses of those persons suspected to be a source;
- Communications addresses of persons suspected to be acting as intermediaries between the journalist and the suspected source;

Any application relating to journalistic sources must be approved by an IPCO Judicial Commissioner in addition to the ODCA authorisation via NAFN. The Applicant should inform the Senior Responsible Office in respect of such applications.

Prepaid Mobile Phones

Subscriber checks on some mobile telephone numbers may reveal that the phone is an unregistered prepaid mobile telephone as these types of phones are used by many criminals to avoid detection. However, in order to gather more information, the Applicant making a request may receive as part of their request for entity data top-up details, method of payment, bank account used or customer notes. The Applicant should outline in their original application the further information that will be required if the phone turns out to be prepaid, so as to allow the widening of the data capture.

The information that is received can then be developed to try to obtain further information about the user of the phone. Solution Providers such as EasyPay, EPay etc, are the third parties involved in the transaction of credit placed on a mobile phone. If a Solution Provider is provided with the mobile telephone number, the transaction date and the transaction number, they are often able to provide the method of payment and the location of the top-up. Solution Providers are not CSPs and therefore the data can be applied for under the Data Protection Act.

Considerations regarding Necessity

In order to justify the application is necessary the applicant needs as a minimum to consider three main points:

- The **event** under investigation, such as a crime or vulnerable missing person;
- The **person** whose data is sought**,** such as a suspect, witness or missing person and how they are linked to the event; and
- The **communications** data sought, such as a telephone number or IP address, and how this data is related to the person and the event;

In essence, necessity should be a short explanation of the investigation, the person and the communications data and how these three link together. The application must establish a link between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

Considerations regarding Proportionality

Applicants should include an outline of how obtaining the data will benefit the investigation or operation. The relevance of the data being sought should be explained as should any information that the applicant is aware of which might undermine the application.

This outline should include explaining how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example the subscriber details of a phone number may be obtained from a phone book or other publically available source.

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

The two basic questions are:

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

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 examination of the proportionality of the application should include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

An examination of the proportionality of the application should also involve consideration of possible unintended consequences and, when relevant this should be noted. Unintended consequences are more likely in applications for events data or in applications for the data of those in professions with duties of confidentiality. For example, if a journalist is a victim of crime, applications for events data related to that journalist’s phone number as part of the criminal investigation may also return some phone numbers of that journalist’s sources, with unintended impact on freedom of expression. Such an application may still be necessary and proportionate but the risk of unintended consequences should be considered.

Considerations regarding Collateral Intrusion

Consideration of collateral intrusion forms part of the proportionality considerations. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion. When there are no meaningful collateral intrusion risks, such as when applying for subscriber details of the person under investigation, the absence of collateral intrusion should be noted.

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 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 cannot identify any meaningful collateral intrusion that factor should be recorded in the application i.e. “none identified”.

Role of the SPOC

The SPOC is an individual trained to facilitate the lawful acquisition of communications data and effective co-operation between a public authority, the OCDA and telecommunications and postal operators. The Home Office must accredit all SPOCs, and this involves attendance on a recognised training course, the passing of an examination and being issued with a SPOC Personal Identification Number. The SPOC ensures that only practical and lawful requests for communications data are undertaken.

Applicants within local authorities are required to consult a NAFN SPOC throughout the application process. The accredited SPOCs at NAFN will scrutinise the applications independently. They will provide advice to the local authority ensuring it acts in an informed and lawful manner.

The SPOC will, as appropriate:

- Assess whether the acquisition of the data is reasonably practicable or inextricably linked to other data;
- Advise on and manage the use of the request filter;
- Advise on the interpretation of the Act, particularly whether an authorisation is appropriate;
- Provide assurance that authorisations are lawful under the Act and free from errors;
- Consider and, where appropriate, provide advice on possible unintended consequences of the application; and
- Assess any cost and resource implications to both the public authority and the CSP of communications data requirements

The OCDA ultimately decides whether to authorise the acquisition of data.

In addition to each application being considered by a NAFN SPoC, the local authority making the application must ensure someone of at least the rank of the senior responsible officer in the authority is aware the application is being made before it is submitted to an authorising officer in OCDA.

Approval of Requests

Section 60A of the Act provides for the independent authorisation of communications data requests by the IPC. The Office of Communications Data Authorisation (OCDA) performs this function on behalf of the IPC.

The OCDA has current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data.

The OCDA will consider the form and then complete the Designated Person's part of the Application Form to state whether they grant or refuse the application. The Designated Person must record on the form:

- Why he/she believes acquiring the communications data is necessary;
- Why he/she believes the conduct involved in acquiring the communications data is proportionate;
- If accessing the communications data involves a meaningful degree of collateral intrusion, why he/she believes that the request is still proportionate;

When considering proportionality the OCDA should apply particular consideration to unintended consequences.

The decision of the OCDA must be based on the information presented to them in the application. If the application is approved the OCDA can authorise the accessing of communications data via the NAFN SPOC.

The OCDA shall endorse the draft notice or authorisation with the date, and if appropriate the time, at which he or she gives the notice or authorisation. This is the point at which the OCDA approves the application.

If the application is rejected by the SPOC or the OCDA, the SPOC will retain the electronic application and inform the applicant in writing of the reasons for its rejection. As with all communication, this will be via via the NAFN website.

Notices and Authorisations

All notices and authorisations should refer to data relating to a specific date or time-period. If the date is specified as "current" the data should be provided by the CSP as at the date of the notice. The notice should give enough information to the CSP to allow them to comply. There is no need to produce a separate notice for each communications address, when these addresses all relate to the same CSP.

The notice is then served on the Communications Service Provider by the SPOC. The SPOC will give the notice a Unique Reference Number that cross-references it to the application that was granted. The SPOC is responsible for all contacts between the Authority and the Communications Service Provider.

Once the data is obtained the SPOC will provide the data to the Applicant, but the SPOC can filter out any unnecessary information provided by the Communications Service Provider. The SPOC will retain the original data obtained from the CSP. The Applicant should keep the data that they receive in a secure manner, in order to comply with data protection requirements.

Under Section 66 of the Investigative Powers Act, the Communications Service Provider must comply with the requirements of a notice, as long as it is reasonably practical for them to do so. Where there are no agreed service levels, the CSP should disclose the required communications data within 10 working days of the notice being served on them.

All notices and authorisations will only be valid for a month, but they may be renewed for further periods of a month, at any time within the current life of the notice or authorisation. This should be set out by the Applicant in an addendum to the original application.

If the need for the communications data ends or its obtaining is no longer proportionate before the provision of this data by the Communications Service Provider, a designated senior officer must cancel the notice. This is done via the NAFN website. However, the notices (and authorisations) terminate when the Communications Service Provider provides the requested data, so there is usually no need for a cancellation form to be completed.

A local authority may not make an application that requires the processing or disclosure of internet connection records.

Errors

Where any error occurs, in the giving of a notice or authorisation or as a consequence of any authorised conduct or any conduct undertaken to comply with a notice, a record should be kept.

There are 2 types of errors namely reportable errors and recordable errors.

- Reportable errors are ones where communications data is acquired wrongly and in this case a report must be made to the Interception of Communications Commissioner, as this type of occurrence could have significant consequences for the individual whose details were wrongly disclosed.
- Recordable errors are ones where an error has occurred but has been identified before the communications data has been acquired. The Authority must keep a record of these occurrences, but a report does not have to be made to the Commissioner.

Reportable Errors could include:

- A notice being made for a purpose, or for a type of data, which the public authority cannot seek;
- Human error, such as incorrect transposition of information where communications data is acquired;
- Disclosure of the wrong data by a CSP when complying with a request under Part 3 of the Act;
- Disclosure or acquisition of data in excess of that required;

Recordable Errors could include:

- A notice which is impossible for a Communications Service Provider to comply with;
- Failure to review information already held, e.g. seeking data already acquired or obtained for the same investigation, or data for which the requirement to obtain it is known to be no longer valid;
- Human error, such as incorrect transposition of information where communications data is not acquired;

Where a telephone number has been ported to another Communications Service Provider then this does not constitute an error. Where excess data is disclosed, if the material is not relevant to the investigation it should be destroyed once the report has been made to the IPC. This should include destroying copies contained as attachments in e-mails. If having reviewed the excess

material it is intended to make use of it, the Applicant must make an addendum to the original application to set out the reasons for needing to use this excess data. The Designated Person will then decide whether it is necessary and proportionate for the excess data to be used in the investigation. The requirements of DPA and its data protection principles must be adhered to in relation to an excess data.

Any reportable error must be reported to the Senior Responsible Officer and then to the IPC within 5 working days. The report must contain the unique reference number of the notice and details of the error, plus an explanation how the error occurred, indicating whether any unintended collateral intrusion has taken place and providing an indication of the steps that will take place to prevent a reoccurrence.

If the report relates to an error made by a Communications Service Provider the Authority must still report it, but should also inform the CSP to enable the CSP to investigate the cause.

The records kept for recordable errors must include details of the error, explain how the error occurred and provide an indication of the steps that have been, or will be, takento prevent a reoccurrence. These records must be regularly reviewed by the Senior Responsible Officer.

The most common cause of errors is the incorrect transposition of telephone numbers, e-mail addresses and IP addresses. In the vast majority of cases these addresses are derived from addresses available to the Applicant in electronic form. Therefore all Applicants are required to electronically copy communications addresses into applications when the source is in electronic form (for example forensic reports relating to mobile phones or call data records etc.) Communications addresses acquired from other sources must be properly checked to reduce the scope for error.

In circumstances where a reportable error is deemed to be of a serious nature and it is in the public interest to do so,the IPC must inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal. The Tribunal has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data.

Senior Responsible Officer

The Senior Responsible Officer is responsible for:

- The integrity of the process in place to acquire communications data;
- Compliance with the Act and Code of Practice;
- Oversight of the reporting of errors to the IPC;
- Engaging with IPC inspectors when they conduct inspections;
- Overseeing the implementation of any post-inspection action plans;

The Director of Legal and Democratic Services is the Senior Responsible Officer with regard to the acquiring of communications data

Records to be Maintained by a Public Authority

Records kept by the public authority (Local Authority) must be held centrally by the SPOC or in accordance with arrangements previously agreed with the IPC. In practice, this means that NAFN will retain all copies of applications, refusals, variations and authorisations.

Records must be available for inspection by the IPC and retained for the IPT to carry out its functions under Part 4 of the Regulation of Investigatory Powers Act. Records are only required to be retained for three years, but it is desirable to retain for five.

It should be noted that there are other statutory obligations places on public authorities in respect of data retention, for example, the disclosure requirements of investigative material within the Criminal Procedure and Investigations Act 1996.

Each public authority must also keep a record of the following information:

- The number of applications submitted seeking the acquisition of communications data;
- The number of applications requiring amendment or declined by the SPOC to the applicant, including the reason for such;
- The number of authorisations of conduct to acquire communications data granted;
- The number of authorisations to give a notice to acquire communications data granted;
- The number of notices given pursuant to an authorisation;
- The priority grading of the authorisations;
- Whether any part of the authorisation relates to a person who is a member of a profession that handles privileged or otherwise confidential information, and if so, which profession;
- The number of items of communication data sought, for authorisation granted

Code of Practice

The Council and those persons acting under of the Act must have regard to the Communications Data Code of Practice issued by the Home Office under the Act. The current version of the Code of Practice is available on the Home Office website.

Annex

Local Authority Communications Data Application Process – Simple Guide

Relevant Person	Action
Applicant	Creates a communications data application on NAFN, including all relevant information including the statutory purpose for the acquisition of the data for the applicable crime purpose On the application, record as part of the necessity case: • A description of the offence(s) under investigation; and • A justification for the seriousness of the offence (record which serious crime definition is met and how it is met, or record that the crime is not serious)
Approved Rank Officer	Reviews the application and verifies on NAFN that the application is appropriate and meets all required criteria Note: This step is only required for local authorities
NAFN SPOC	Checks that the public authority is permitted to use the recorded statutory purpose Determines the conduct to satisfy the applicant's need (the type of data that is required) If event data is required and the statutory purpose is crime, checks the applicant has recorded: • A description of the offence(s) • A justification for the seriousness of the offence(s) If not, the application is returned for rework
OCDA	Provides an independent authorisation of communications data applications on behalf of the Investigatory Powers Commissioner (IPC) Checks and records that the applicant: • Has fully considered and understood the application • Has understood and considered necessity • Has considered the potential for the authorisation to result in unintended consequences, such as collateral intrusion Facilitates communication with the Communication Service Provider to fulfil the application request, generally via the SPOC
NAFN SPOC	Makes the communication data request of the CSP Takes receipt of relevant communication data, and disseminates to applicant