monmouthshire
sir fynwy

REGULATION OF INVESTIGATORY POWERS ACT 2000

Directed Surveillance, Use of Covert Human Intelligence Sources and Obtaining Communications Data

CONTENTS

PART I – INTRODUCTION

1. Parliament creates laws within which society in all its guises operates. Those laws apply to local authorities (LAs), some of which enable functions, some of which bound functions, and some of which are delegated to them to enact and enforce.

2. The Regulation of Investigatory Powers Act 2000 (as amended) is designed to create the correct tension between allowing LAs to operate in an effective way on behalf of their citizens, and limit that operation with respect to Human Rights (HR), legality and fairness.

3. RIPA covers the acquisition and disclosure of communications data (Part I of RIPA); the carrying out of surveillance and use of covert human intelligence sources (CHIS) (Part II); and the investigation of electronic data protected by encryption (Part III).

4. In accordance with sections 28 and 29 of the Act, Monmouthshire County Council (MCC) is empowered to make use of the practices set out in Part II. It would potentially do so as part of its duty to tackle illegal practice. Examples of which may include fly-tipping, selling counterfeit or dangerous goods, animal cruelty, fraud, underage sales of alcohol – the list is non-exhaustive. MMC is permitted to:

    a. carry our directed surveillance. This is the planned, covert 'watching' of someone or somewhere that is likely to result in the obtaining of information about a person;

    b. carry out CHIS activity. This is the establishment of a relationship that is used covertly to obtain or disclose information.

5. In fulfilling its functions, MCC must comply with a framework of legislation that includes:

    a. Human Rights Act 1998;

    b. Regulation of Investigatory Powers Act 2000;

    c. Protection of Freedoms Act 2012;

    d. Investigatory Powers Act 2016;

    e. Data Protection Act 2018;

    and the broad sweep of criminal legislation and common law.

6. This policy talks to the use of surveillance and covert human intelligence sources (CHIS) MCC is not permitted to carry out:

    a. intrusive surveillance;

    b. entry onto or interference with property;

    c. interception of communications;

    d. any other surveillance-related activity not covered by Part II of RIPA.

AIM

7. This policy sets out to:

a. explain what RIPA is and how MCC interacts with it;

b. explain what MCC can and can't do;

c. explain the legislative framework within which MCC must operate;

d. signpost the reader to the correct guidance relating to RIPA:

e. signpost the reader to the most up-to-date resources, templates and materials to be used whenever RIPA applies;

f. set out who within MCC may make use of the practices that RIPA bounds;

g. establish a resource and framework so that the whole authority is informed about RIPA;

h. prevent inadvertent use of techniques or practices that should fall under RIPA;

i. ensure that MCC operates legally.

And it should be read in conjunction with the RIPA Authorisation, Training and Review plan that is maintained by the SRO in the RIPA site. This subservient document is a 'live' document that sets out who is suitably trained and experienced to carry out activities covered by this policy, a training schedule and a programme of review and consultation.

THE LAW

8. MCC has a duty across myriad different areas of operation and legislation to apply and uphold the law. This could be the protection of children, animals, the consumer, visitors, vulnerable people – in short, everyone.

9. Some of this duty is exercised under the prescription of the law. So it may be that a criminal law is requires MCC to take an individual to Court, family law requires MCC to intervene in the case of a neglected child, licensing law requires MCC to consider the suitability of an individual to drive a taxi – again, this is very broad.

10. And then there is the use of the law in establishing information that will ultimately determine what the outcome of the above will be. It may be witnesses appearing in Court to explain how an animal came to be injured, it may be that access to an establishment is approved in order to assess the hygiene of food preparation – you are hopefully getting a feel for how this works.

11. But these duties and powers and bounded. Each in turn will have systems and processes that prevent misuse or abuse. And there are the overarching facets of Human Rights legislation that always apply:

    a. Article 6 ensures that when a legal process is pursued that the individual has a fair trial with all that this entails regarding the obtaining of evidence and opportunity to challenge it;

    b. Article 8 establishes the individual's right to a private life, and so limits the extent the State, in any guise, may impinge on that and creates a just tension between the exercise of MCC's duties with consideration for the individual;

    c. Article 14 ensures that in the pursuit of MCC's duties that it does it in a non-discriminatory way.

12. And this is where RIPA, IPA and the framework of Commissioners, training, guidance and inspection come in: to ensure that MCC is capable of carrying out its functions and duties, but that it does it a bounded and legal way.

13. The essence of finding the right balance between these different pieces of legislation is acting in a way that is **necessary** and **proportionate**. Those 2 watchwords must sit at the heart of how the reader of this policy acts, embellished by correct training, knowledge and communication.

ROLES AND RESPONSIBILITIES

14. Elected Members. Cabinet is responsible for any RIPA policy and Governance and Audit Committee will be presented annually with an update regarding RIPA within the organisation. This is not just to monitor when it has been used but also to ensure that there is no inadvertent activity relating to RIPA powers.

15. Senior Responsible Officer (SRO). The SRO is the Chief Officer Law and Governance. In circumstances where they are unable to carry out the role of SRO, the outgoing or current chief officer can with the agreement of the Chief Executive appoint a solicitor in the Legal team with suitable knowledge and experience in RIPA to serve as acting SRO. The SRO is responsible for:

    a. the integrity of the RIPA framework and process within MCC;

    b. compliance with Part II of RIPA and with the relevant codes;

    c. engagement with the Commissioners and inspectors when they conduct their inspections, and where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner;

    d. overseeing and co-ordinating the:

        i. submission of annual reports detailing RIPA activity and oversight to the Audit and Governance Committee;

        ii. the identification of issues in the oversight process, to enable analysis of issues, evidencing results, and ensuring subsequent feedback into the RIPA training, to ensure these matters are corporately addressed;

        iii. training needs of the organisation;

        iv. dissemination of guidance and information as required.

16. Authorising Officers (AOs). They are responsible for:

    a. receiving and assessing **all** applications to carry out RIPA activity;

    b. applying the criminal threshold established by the 2012 Act when considering such applications;

    c. the application of all legislative and Home Office guidance tests and bets practice in support of assessing what is reasonable and proportionate in all the circumstances;

    d. providing guidance and oversight to professional applicants in all RIPA related matters;

e. working with the SRO to establish training requirements and carry out reviews as required;

f. as with applications, applying the same rigour and standards to the tracking and completion of all reviews, renewals and cancellations.

17. Gatekeepers. These are suitably experienced and senior line managers capable of assisting Professional Applicants in the drafting of applications such that the AO can be satisfied that due diligence has taken place.

18. Professional Applicant. This is the Officer with the most knowledge of any particular matter who is best placed to complete the application and subsequent review, renewal or cancellation paperwork for submission to the AO and the Court when required.

17. Magistrates' Court. Judicial approval for the use of LA powers is required in accordance with the legislation.

18. Investigatory Powers Commissioner's Office. The team overseen by the independent Commissioner dedicated to fulfilling the duties placed upon them by the 2016 Act. For the purposes of MCC this is the organisation that will inspect and recommend best practice, collate statistical data and, when required, take action relating to bad practice.

REFERENCE

19. Various pieces of legislation are listed above and there is also a considerable amount of guidance and best practice available, as well as training materials accumulated over time, past inspection reports, template documents and the central record of authorisations.

20. All of these documents can be found at the MCC RIPA site for those granted access. It is imperative that full use of the information and documentation available in this resource is made every time an operation is considered, or when it is suspected that there may be activity underway that may classify as RIPA activity inadvertently.

21. No one should be carrying out any RIPA activity without first making use of the Home Office Codes of Practice on Covert Surveillance and Property Interference (August 2018) and Covert Human Intelligence Sources (December 2022).

PART II – SURVEILLANCE

22. Part II of RIPA sets out a regulatory framework for the use of covert investigatory techniques by LAs.

WHAT IS SURVEILLANCE?

23. Surveillance is:

    a. monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

    b. recording anything monitored, observed or listened to in the course of surveillance;

    c. by or with the assistance of appropriate surveillance device(s).

    It can be overt or covert.

24. Overt Surveillance. This is generally how MCC will carry out investigations. There will be nothing secretive or clandestine and, in many ways, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), or will be going about Council business openly (e.g. a market inspector walking through markets).

25. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that Officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met).

COVERT SURVEILLANCE

26. Covert Surveillance is defined in s26(9)(a) RIPA:

    "*Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place*".

27. General observation forms part of the duties of many enforcement officers. Such observation may involve the use of equipment or merely reinforce normal sensory perceptions, such as binoculars or the use of cameras, where this does not involve systematic surveillance of an individual. It forms part of the everyday functions of law enforcement or other public bodies. This low level activity will not usually be regulated under the provisions of RIPA.

28. The installation of CCTV cameras for the purpose of generally observing activity in a particular area is not surveillance which requires authorisation. Members of the public are aware that such systems are in use, for their own protection and to prevent crime.

29. However, an authorisation may be required if a CCTV camera is to be used for surveillance as part of a specific investigation or operation otherwise than as an immediate reaction to events. In such circumstances either the Council or the police may give the necessary authorisation. If an authorisation is given by the police then a record of the authorisation will be kept to ensure any surveillance is within its terms.

30. Part II of RIPA applies to the following conduct:

a. directed surveillance;

b. intrusive surveillance; and

c. the conduct and use of covert human intelligence sources (CHIS).

DIRECTED SURVEILLANCE

31. Directed Surveillance is defined in s26(2) RIPA:

"…*surveillance is directed for the purposes of this Part if it is covert but not intrusive and is undertaken:*

(a) for the purposes of a specific investigation or a specific operation;

(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance."

32. Where it is anticipated that mobile surveillance will be an integral part of any directed surveillance operation Authorising Officers must be satisfied that it is necessary and the need is proportionate to the investigation being undertaken. Mobile surveillance is a specialist skill and should, at all times, be assessed for risks to health and safety of operatives engaged in this activity. At no times should road traffic laws or regulations be ignored by officers engaged in mobile surveillance. Due regard should be afforded to the driving and surveillance skills of operatives engaged in such activity. Under no circumstances will officers engage in high-speed pursuit of vehicles involved in Directed Surveillance operations.

33. Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'), is planned, this could amount to direct (or even intrusive) surveillance and there will be a requirement to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude.

34. The general observation duties of many law enforcement officers and other public authorities do not require authorisation under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people.

35. Private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

36. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis.

INTRUSIVE SURVEILLANCE AND CONFIDENTIAL INFORMATION

37. Intrusive Surveillance is defined in s26(3) RIPA:

"Subject to subsections (4) to (6), surveillance is intrusive for the purposes of this Part if, and only if, it is covert surveillance that—

(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device."

38. MCC cannot, by law, conduct intrusive surveillance. It also cannot obtain information of a confidential nature such as a client speaking to their lawyer, journalistic material and relevant personal information.

INTERFERENCE WITH PROPERTY

39. This is covered by other legislation and MCC is not permitted to undertake this activity.

PART III – COVERT HUMAN INTELLIGENCE SOURCE

40. This is defined in s26(8) of RIPA:

"...a person is a covert human intelligence source if –

(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship."

41. The concept of "covertness" is very similar to that used in relation to directed surveillance. Here, however, it is used at 2 stages, both of which must be met for an authorisation to be required:

a. the covert purpose of the relationship;

b. the covert actions of obtaining or providing access to information and of disclosing such information.

42. If a person has a relationship with another person which is not established or maintained for a covert purpose, the fact that he or she does in fact covertly disclose information to the local authority will not require an authorisation and that person will not be a CHIS.

43. There is no use of CHIS merely because a person offers information to the local authority that may be material to the investigation of an offence, but there would be if the authority asks the person to obtain further information. It is important that what starts out as a member of the public offering information does not evolve into a CHIS relationship by MCC seeking to develop a relationship to gather more information.

44. A CHIS is somebody who is concealing or misrepresenting their true identity or purpose in order to covertly gather or provide access to information from the target. Examples of a CHIS include a private investigator pretending to live on a housing estate to gather evidence of drug dealing or an informant who gives information to Trading Standards about illegal business practices in a factory or shop.

USING A CHIS

45. Section 29(5) sets out a number of definitive requirements:

a. there will at all times be an officer within the local authority who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security and welfare;

b. there will at all times be another officer within the local authority who will have general oversight of the use made of the source;

c. there will at all times be an officer within the local authority who has responsibility for maintaining a record of the use made of the source;

d. the records relating to the source maintained by the local authority will always contain particulars of all matters specified by the Secretary of State in Regulations. (The current

regulations are The Regulation of Investigatory Powers (Source Records) Regulations 2000). These particulars are:

i. the identity of the source;

ii. the identity, where known, used by the source;

iii. any relevant investigating authority other than the authority maintaining the records;

iv. the means by which the source is referred to within each relevant investigating authority;

v. any other significant information connected with the security and welfare of the source;

vi. any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph iv. has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

vii. the date when, and the circumstances in which, the source was recruited;

viii. the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the Act (see bullet points above) or in any order made by the Secretary of State under section 29(2)(c);

ix. the periods during which those persons have discharged those responsibilities;

x. the tasks given to the source and the demands made of him in relation to his activities as a source;

xi. all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

xii. the information obtained by each relevant investigating authority by the conduct or use of the source;

xiii. any dissemination by that authority of information obtained in that way; and

xiv. in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority;

e. that records maintained by the local authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

46. These requirements make it very unlikely that an investigation could involve the use of a CHIS without there having been prior planning within the investigating department/section. It is important to realise that it may well be a member of staff of the department and, indeed, an investigator him or herself, who becomes the source, depending on the manner of working

used. It is not only persons outside the employ of the local authority who may be used as a source.

47. MCC will not carry out any operations involving a CHIS without specific and up to date training of those officers involved with any of the duties set out at para 45.

48. No CHIS is to engage in any criminal activity in the course of their operation.

JUVENILES AND VULNERABLE PERSONS AS CHIS

49. This is governed by the Regulation of Investigatory Powers (Juveniles) Order 2000. A person under 16 cannot be used as a CHIS if the relationship that would be covertly used is between the juvenile and his/her parent or person with parental responsibility for him/her. (Whether or not a person who is not a parent has parental responsibility for a child may only be determined by having sight of documentation, e.g. a court order providing for that person to have parental responsibility. Further, a person may have parental responsibility for a juvenile, even though they no longer live together).

50. The Regulations also provide in the case of a source under 16 that there is at all times a person within the local authority responsible for ensuring that an appropriate adult (parent or guardian, any other person who has assumed responsibility for the juvenile's welfare, or where there are no such persons, any responsible person over 18 who is not a member or employee of the local authority – therefore a local authority social worker is not eligible to act as appropriate adult) is present at meetings between the juvenile source and any person representing the investigating authority.

51. Where the source is under 18, authorisation may not be granted or renewed unless there has been made or updated a risk assessment sufficient to demonstrate that the nature and magnitude of any risk of physical injury or psychological distress to the juvenile arising out of his or her use as a source has been identified and evaluated.

52. The Authorising Officer must have considered the risk assessment and satisfied him/herself that the risks are justified and have been properly explained to and understood by the source. The Authorising Officer must also be clear whether or not the covert relationship is between the juvenile and any relative, guardian or person who has assumed responsibility for his/her welfare and, if it is, has given particular consideration to whether the authorisation is justified ("necessary" and "proportionate") in the light of that fact.

53. A vulnerable person is or may be in need of community care services by reason of mental or other disability, age, illness or is unable to take care of themselves or unable to protect themselves against significant harm or exploitation.

54. Any such individual should only be used as a source in the most exceptional circumstances and the SRO must be involved in any decision relating to this category of person.

CHIS RECORD KEEPING

55. Records should be kept as prescribed by the Code of Practice. Where a source wearing or carrying a surveillance device is invited into residential premises or a private vehicle and records activity taking place inside those premises or vehicle, authorisation for use of that covert source should be obtained in the usual way.

56. The source should not use an invitation into residential premises or private vehicle as a means of installing equipment. If equipment is to be used other than in the presence of the covert

source, an intrusive surveillance authorisation is necessary which cannot be granted by the local authority.

PART IV – COMMUNICATIONS DATA AND NON-RIPA SURVEILLANCE

COMMUNICATIONS DATA

57. MCC is permitted to acquire information defined as "communications data". This includes subscriber data and service data but not "traffic data" as defined by the Act. MCC is a member of the National Anti Fraud Network (NAFN).

58. Communications data is "*information held by communication service providers (e.g. telecom, internet and postal companies) relating to the communication made by their customers*". This includes information relating to the use of a communications service but does not include the contents of the communication itself.

59. Communication data is broadly split into 3 categories:

    a. s21(4)(a) - "traffic data"; This is usually data generated by the Communications Service Provider (CSP) in the process of delivering a communication. (Not included in Local Authority authorisation);

    b. s21(4)(b) - server use or billing information - the use made of the service by any person i.e. itemised telephone records; e.g. numbers called, itemised connection records, itemised timing and duration of services, connection, disconnection and reconnection information; provision and use of forwarding/redirecting services; conference calls call messages call waiting & call baring information;

    c. s21(4)(c) - postal records including records of registered, recorded or special delivery postal items.

60. In the context of telephone data, it would include the telephone numbers of the phone from which the call was made and the number of the phone receiving the call. It also includes the date, time, duration and place of the call. It does not include the actual content of the telephone call.

61. In respect of e-mail and the internet, it would include details of the subscriber account. It would also include dates and times when e-mails have been sent or received. The content of the e-mails are excluded from communications data. The websites are included but not the actual web pages that have been viewed.

62. In the context of a letter, it would include the information on the envelope but not the contents of the letter. The information will therefore include the name and address of the recipient and the postmark showing when and where the letter was sent. It might also contain details of the address of the sender if recorded on the envelope.

63. MCC is not permitted to carry out the interception of any communications data. There may be situations where either the caller or receiver consents to the recording of the telephone conversation and, in such circumstances a warrant is not required. This type of surveillance will require authorisation, either as directed covert surveillance, or, if it is a CHIS making or receiving the telephone conversation (usually an officer working "undercover"), as a CHIS authorisation.

64. Where as part of an already authorised directed covert surveillance or CHIS a telephone conversation is to be recorded by the officer or the CHIS then no special or additional authorisation is required.

65. The recording of telephone conversations for purposes not connected with investigatory powers does not fall within the RIPA legislative framework.

EMPLOYEES

66. s1 of RIPA does not apply to Local Authorities except where the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 - SI2000/2699 applies. The legislative framework permits the Council without further authorisation to lawfully intercept its employees' e-mail or telephone communications and monitor their internet access for the purposes of prevention or detection of crime or the detection of unauthorised use of these systems.

NON-RIPA SURVEILLANCE

67. MCC may occasionally wish to undertake covert surveillance which is not regulated by RIPA. This would be an activity not considered a 'core' function, and instead a 'normal' function, ie. something common to all organisations such as the investigation of an employee moonlighting. The 2018 Guidance relating to non-core functions should be consulted in this situation.

68. Similar mechanisms for activity which cannot be protected by the 2000 Act is encouraged. The human rights aspects must still be considered alongside legislation such as the Data Protection Act 2018 and guidance issued by the ICO.

69. An authorisation process provides a useful audit of decisions and actions. The process reflects that of directed surveillance, save for the Judicial approval.

70. Authorisation under RIPA affords a public authority a defence under s27 i.e. the activity is lawful for all purposes, provided an authorisation is in place, and the conduct of the officers is in accordance with the legislation. However, failure to obtain an authorisation does not make covert surveillance unlawful.

71. Section 80 of RIPA contains a general saving for lawful conduct. RIPA is a shield not a sword.

CCTV

72. Normal use of CCTV is governed by the MCC CCTV Strategy and associated documents.

73. CCTV only falls under the umbrella of RIPA when it is used in such a way to satisfy the tests set out in the introduction, ie. a pre-planned use of directed surveillance for the purpose of obtaining private information.

PART V – SOCIAL MEDIA

74. It is important to be aware that use of social media in an investigation could, depending on how it is used and the type of information likely to be obtained, constitute covert activity that requires authorisation under RIPA.

75. Generally, researching 'open source' material would not require authorisation, but return visits in order to build up a profile could change the position – this may constitute directed surveillance depending on the circumstances. Examples of 'open source' material, are materials you could view on social media without becoming a friend, subscriber or follower.

76. The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed.

77. Where it is intended to access a social media or other online account to which the Council has been given access with the consent of the owner, the Council will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

78. Officers should not use false personae (eg. a false Facebook profile or X (formerly Twitter) handle) to disguise their online activities. False personae should not be used for a covert purpose without authorisation.

79. In order to determine whether an authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. The guidance at paras 3.10-3.17[1] and 4.29-4.35[2] in the Home Office Codes of Practice should be consulted. Factors that should be considered in establishing whether a directed surveillance authorisation is required include whether:

    a. the investigation or research is directed towards an individual or organisation;

    b. it is likely to result in obtaining private information about a person or group of people;

    c. it is likely to involve visiting internet sites to build up an intelligence picture or profile;

    d. the information obtained will be recorded and retained;

    e. the information is likely to provide an observer with a pattern of lifestyle;

    f. the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;

    g. the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

[1] Home Office Code of Practice on Covert Surveillance and Property Interference, August 2018
[2] Home Office Code of Practice on Covert Human Intelligence Sources, December 2022

h. it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

PART VI – SAFEGUARDS, ERRORS, COMPLAINTS AND DATA RETENTION

SAFEGUARDS

80. Material obtained through surveillance may include private information, legally privileged information, or other confidential material including journalistic material and constituency business of Members of Parliament.

81. Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. Something is necessary for the authorised purposes where the material:

    a. is (or is likely to become) necessary for the surveillance purposes set out in the legislation;

    b. is necessary for facilitating the carrying out of the functions of the Council under the surveillance legislation;

    c. is necessary for facilitating the carrying out of any functions of the Commissioner or Investigatory Powers Tribunal;

    d. is necessary for the purposes of legal proceedings;

    e. is necessary for the performance of the functions of any person by or under any enactment.

82 When information obtained under a surveillance authorisation is used evidentially, the Council should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

83. Regular reviews of all authorisations should be undertaken during their lifetime to assess the necessity and proportionality of the conduct. Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or particularly sensitive information is likely to be obtained.

84. The Council will likely need to share information obtained through surveillance within the Council and between the Council and other public bodies where legally necessary. This must be limited to the minimum necessary. If a summary of the information will be sufficient to meet necessity, no more than that should be disclosed.

85. When sharing this type of information MCC will ensure that it has appropriate safeguards and agreements in place to ensure compliance.

86. Information and material obtained through surveillance must only be copied to the extent necessary. Copying includes direct copies as well as summaries and extracts.

87. All information and material obtained through surveillance and all copies, extracts or summaries must be stored securely to minimise the risk of theft or loss. Only those with appropriate legal authority and security clearance should be able to access the information.

88. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relates to his or her physical or mental health or to spiritual counselling. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or any legal obligation of confidentiality. For example, confidential

personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

89. Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency business. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

90. The reasons for acquiring information of this type must be clearly documented and the specific necessity and proportionality of doing so must be carefully considered.

91. Material which has been identified as confidential personal or confidential constituent information should be retained only where it is necessary and proportionate to do so in accordance with the authorised purpose or where otherwise required by law. It should be securely destroyed when its retention is no longer needed for those purposes.

92. Where confidential personal or constituent information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from the SRO.

93. Any case where confidential personal or constituent information is retained, other than for the purpose of destruction, and disseminated should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and any material which has been retained should be made available to the Commissioner on request so that the Commissioner can consider whether the correct procedures and considerations have been applied.

94. There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists in confidence.

95. Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking. Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist nor the source (for example, a news editor who has been sent some notes by a journalist).

96. An application for authorisation where the purpose, or one of the purposes, of the authorisation is to authorise the acquisition of material of this type must contain a statement in those terms. The person to whom the application is made may issue the authorisation only if they consider that appropriate safeguards relating to the handling, retention, use and disclosure of the material are in place.

97. When this type of material is retained and disseminated to an outside body, reasonable steps should be taken to mark it as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of such information, advice should be sought from a legal adviser to the Council before any further dissemination of the content takes place.

98. Where this type of information has been obtained and retained, other than for the purposes of destruction, the matter should be reported to the Commissioner as soon as reasonably practicable.

99. The acquisition of material subject to legal privilege is particularly sensitive and is

therefore subject to additional safeguards which provide for three different circumstances where legally privileged items will or may be obtained. They are:

a. where privileged material is intentionally sought;

b. where privileged material is likely to be obtained;

c. where the purpose or one of the purposes is to obtain items that, if they were not generated or held with the intention of furthering a criminal purpose, would be subject to privilege.

100. The 2010 Legal Consultations Order provides that surveillance that is carried out in relation to anything taking place on so much of any premises specified in article 3(2) of the Order as is, at any time during the surveillance, used for the purposes of 'legal consultations', shall be treated for the purposes of Part II of RIPA as intrusive surveillance. As a result, such authorisations are not available to the Council.

101. Where a lawyer, acting in this professional capacity, is the subject of surveillance, it is possible that a substantial proportion of any material which will or could be acquired will be subject to legal privilege. In addition to considering the applicability of the 2010 Legal Consultations Order, the Council will need to consider which of the three circumstances that apply when items subject to legal privilege will or may be obtained is relevant, and what processes should therefore be followed.

102. Any case involving lawyers' material should also be notified to the Commissioner during their next inspection, and any material which has been retained should be made available to the Commissioner on request.

ERRORS

103. Regular reviews of errors will be undertaken with a written record made of each review.

104. An error must be reported if it is a "relevant error", which is defined under section 231(9) of the IPA as being any error by MCC in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of RIPA. Examples of relevant errors occurring would include circumstances where:

a. surveillance or Covert Human Intelligence Source activity has taken place without lawful authority;

b. there has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Codes.

105. All relevant errors made by the Council of which it is aware must be reported to the IPC as soon as reasonably practicable, and no later than 10 working days (or as agreed with the Commissioner). Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

106. From the point at which the Council identifies that a relevant error may have occurred, it must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the Council must also inform the Commissioner of when it was initially identified that an error may have taken place.

107. The report should include information on the cause of the error; the amount of surveillance conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

108. The IPC may issue guidance as necessary, including guidance on the format of error reports. The Council must have regard to any guidance on errors issued by the IPC.

SERIOUS ERRORS

109. If the IPC considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error, they must inform them. An error is a serious error where it is considered to have caused significant prejudice or harm to the person concerned.

110. In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must in particular consider:

a. the seriousness of the error and its effect on the person concerned;

b. the extent to which disclosing the error would be contrary to the public interest or prejudicial to:

i. national security;

ii. the prevention or detection of serious crime;

iii. the economic well-being of the United Kingdom;

iv. the continued discharge of the functions of any of the security and intelligence services.

111. Before making a decision, the Commissioner will ask MCC to make submissions on the matters concerned, and the Council must take all such steps as notified to help identify the subject of a serious error.

112. When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

BREACH OF RIPA

113. Evidence gathered where RIPA has not been complied with may not be admissible in Court and could lead to a challenge under Article 8 of the Human Rights Act.

114. Any perceived breach of this policy or the RIPA procedures should be reported to the Monitoring Officer in order to notify the Investigatory Powers Commissioner immediately.

COMPLAINTS

115. The Council will maintain the standards set out in this guidance and the current Codes of Practice. The Investigatory Powers Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by the legislation.

116. Contravention of the RIPA or the IPA (and associated legislation) may be reported to MCC via the normal corporate complaints policy here: https://www.monmouthshire.gov.uk/feedback/

117. Alternatively, you may contact the IPC directly at:

Investigatory Powers Commissioner's Office
PO Box 29105
London
SW1V 1ZU

Email: info@ipco.org.uk
Telephone: 0207 389 8999

118. Contravention of the Data Protection Act 2018 and/or GDPR may also be reported to the Information Commissioner.

DATA RETENTION

119. Information obtained as the result of any RIPA activity will be retained dependant on the nature of the information.

120. Any information obtained in error, that is collateral and unrelated to the aim, that accidentally goes beyond the scope of the authorisation given or is in breach of law will be destroyed immediately.

121. All other information will be retained for a period of 6 years either from a decision to not pursue any action, or the completion of any related evidential process (eg. a criminal Court case.)

122. This is in accordance with the MCC retention schedule at this intranet link. It complies with the Limitation Act 1980 and aligned with the statute of limitation relating to any subsequent cases relating to a Tort and MCC's policy relating to casefiles.

PART VII – AUTHORISATION PROCESS

123. There is complexity and nuance throughout the process, both leading up to, during, and after any operation that involves RIPA. As such, this section is intended as the starting point for anyone involved in the process, but no one should act in isolation of the Home Office guidance and training materials contained in the MCC RIPA site, and full use of the gatekeepers and Litigation Solicitor should be made.

124. All of the forms required for the different processes are available at the resource above, linked to the latest version online, and are not replicated here. A record of all activity will be maintained in the Central Record of Authorisations (CRA) hat is held in the MCC RIPA site. This will record the key details associated with each application but will not contain any personal information. The applications themselves will be retained by the applicant, and any information obtained from any operation will be retained as per the retention schedule set out in this document.

DIRECTED SURVEILLANCE

125. The Protection of Freedoms Act 2012 amended RIPA 2000 to the effect that authorisation of the use of certain covert powers, including the use of directed surveillance, will only have effect once an order approving the authorisation has been granted by a Magistrates' Court.

126. The assessment of necessity and proportionality throughout is key, and should be evident through the completion of all application/other forms, the consideration given by the AO and the presentation to the Court.

127. All applications for authorisation of Directed Surveillance must be in writing and record:

a. the grounds on which authorisation is sought. For MCC this will be for the prevention and detection of crime and disorder only

b. an assessment of the Directed Surveillance Crime Threshold. Directed surveillance can only be authorised under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or where the investigation is in regard to the underage sale of alcohol or tobacco (see below);

c. consideration of why the Directed Surveillance is proportionate to what it seeks to achieve;

d. what other options for the gathering of information have been considered and that Directed Surveillance is necessary;

e. the nature of the surveillance;

f. the identity or identities, where known, of those to be the subject of Directed Surveillance;

g. the action to be authorised and level of authority required;

h. an account of the investigation or operation;

i. an explanation of the information which it is desired to obtain as a result of the authorisation;

j. any potential for collateral intrusion and why such intrusion is justified;

k. the likelihood of acquiring any confidential or privileged material, and the details of such material;

l. where the purposes include obtaining information subject to legal privilege, as an explanation as to why there are exceptional and compelling circumstances that make this necessary.

128. Where, at any point in an operation, the parameters of the original authorisation are likely to be exceeded, they must inform the applicant and the AO immediately, for example if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. Where the original authorisation is not sufficient separate authorisation is required.

129. The AO must satisfy themselves that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve. It is important that sufficient weight is attached to considering whether the surveillance required is proportionate by:

a. balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

b. explaining how and why the methods adopted will cause the least possible intrusion on the subject and others;

c. considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

d. evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

130. The AO must be able to produce evidence that the relevant issues have been considered for monitoring purposes, for example a note of the documents and information available to the officer at the time the authorisation is given, together with a note of the date and time authorisation was given. It is essential that the AO considers each request for an authorisation on its merits and a rubber stamping approach must never be used.

131. Particular consideration should be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

JUDICIAL APPROVAL

132. Where an Authorising Officer has granted an authorisation (for Directed Surveillance), the authorisation is not to take effect until a Magistrates' Court has made an order approving the grant of the authorisation.

133. The Court will only give approval to the granting of an authorisation for Directed Surveillance if they are satisfied that:

a. at the time the AO granted the authorisation, there were reasonable grounds for believing that the authorisation was necessary and that the surveillance being authorised was proportionate;

b. the AO was a designated person for the purposes of s28 of RIPA;

c. the grant of the authorisation was not in breach of any restrictions imposed by virtue of s30(3) of RIPA;

d. any other conditions provided for by any Order were satisfied;

e. there remain reasonable grounds for believing that the necessary and proportionate tests are satisfied.

134. If a Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

135. No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates' Court of that authorisation has been obtained.

136. AOs must, as early in the process as possible, inform the SRO or Litigation Solicitor in order that arrangements for an application to be made by the Council's lawyers or an appropriate officer to the Magistrates Court for an order to approve the authorisation can be made.

137. The Court does not need to consider cancellations or internal reviews.

138. As a minimum, the Court is to be provided with a copy of the original RIPA authorisation form and the supporting documents setting out the case. This forms the basis of the application and should contain all information that is relied upon. Further, a partially completed judicial application/order form is required.

TIMELINE OF AN AUTHORISATION

139. A written authorisation for Directed Surveillance will cease to have effect at the end of a period of 3 months beginning with the day on which it took effect.

140. If at any time before an authorisation would cease to have effect, the AO considers it necessary for the authorisation to continue for the purpose for which it was given, he/she may approve a renewal in writing for a further period of 3 months, beginning with the day when the authorisation would have expired but for the renewal.

141. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

142. All requests for the renewal of an authorisation for Directed Surveillance must record:

a. whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

b. the information required in the original request for an authorisation plus:

i. any significant changes to the information in the previous authorisation;

ii. why it is necessary to continue with the surveillance;

iii. the content and value to the investigation or operation of the information so far obtained by the surveillance;

iv. an estimate of the length of time the surveillance will continue to be necessary.

143. Renewals of authorisations will also be subject to approval by the Magistrates' Court. The AO must therefore advise the SRO immediately when they are minded to grant a renewal.

144. Applications for renewals should not be made until shortly before the original authorisation period is due to expire but officers must take account of factors which may delay the renewal process (eg. intervening weekends or the availability of the AO).

145. The AO must cancel an authorisation if he/she is satisfied that the Directed Surveillance or the conduct of the CHIS no longer meets the criteria for authorisation. When cancelling an authorisation, an Authorising Officer must ensure that proper arrangements have been made for the activity's discontinuance, including the removal of technical equipment, and directions for the management of the product. Further, where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and risk assessments maintained. In the context of CHIS the AO will want to satisfy themselves that all welfare matters are addressed, and should make appropriate comment in their written commentary.

146. Authorisations for Directed Surveillance, and any subsequent renewals and cancellations, are subject to review by the Government appointed Investigatory Powers Commissioner.

147. AOs will review all Directed Surveillance and CHIS applications and authorisations that they have granted regularly to assess whether they remain necessary and proportionate. The results of a review should be recorded on the appropriate form, and kept in the central record of authorisations. The AO should determine how often the review should take place. This should be done as frequently as is considered necessary and practicable, but not later than once a month following the date of authorisation; sooner where the surveillance provides access to confidential material or involves collateral intrusion.

148. Reviews must record:

a. whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

b. any significant changes to the information in the previous authorisation;

c. why it is necessary to continue with the surveillance;

d. the content and value to the investigation or operation of the information so far obtained by the surveillance;

e. an estimate of the length of time the surveillance will continue to be necessary.

149. All documentation regarding Directed Surveillance should be treated as confidential and should be kept accordingly.

150. Each Service Department undertaking Directed Surveillance must ensure that adequate arrangements are in place for the secure handling, storage and destruction of material obtained through the use of covert surveillance.

151. There is nothing in the 2000 Act which prevents results obtained through the proper use of the authorisation procedures from being used on other Council Department Investigations. However, the disclosure outside of surveillance results obtained by means of covert surveillance and its use for other purposes should be authorised only in the most exceptional circumstances.

Before doing so the AO must be satisfied that the release of material outside of the Council, complies with and meets Human Rights Act requirements.

152. Quarterly review meetings will be held between the SRO, AOs and Gatekeepers at which document retention will be discussed.

153. All refusals to grant authority to undertake Directed Surveillance must be recorded and retained for inspection.

CHIS

154. Much of the above process is applicable to CHIS applications as well. The following should be read in conjunction with the process for DS accordingly.

155. The standards of necessity and proportionality are the same, taking into account the added human complexity and increased chance of collateral intrusion in a CHIS operation. A risk assessment for collateral inclusion is therefore required.

156. The approach taken by the AO is the same, as is the need for a Magistrates' Court to approve any operation.

157. The AO must be satisfied that arrangements exist for the proper oversight and management of the source that satisfy the requirements of s29(5) of the Act and such other requirements as may be imposed by order made by the Secretary of State.

158. There are important welfare provisions attached to any CHIS authorisation. They should fall broadly into line with the approach that MCC takes for the welfare of its staff, recognising the duty of care to covert sources and the importance of a risk with regard to the welfare of the source. The risks to the source may not only be physical but also psychological.

159. The source is not to engage in criminal activity (excluding activity that would be criminal but rendered lawful by authority under the Act – eg. the lawful interception of communications).

160. Conduct of the CHIS:

a. any conduct that is comprised in any such activities as are specified or described in the authorisation; and

b. any conduct by or in relation to the source specified or described in the authorisation; and

c. which is carried out for the purposes of or in connection with the investigation or operation that is specified or described.

161. Court approval is required as per above. Approval of an authorisation for use of a CHIS will only be forthcoming if the Court is satisfied that:

a. at the time the AO granted the authorisation, there were reasonable grounds for believing that the authorisation was necessary;

b. the activity being authorised was proportionate;

c. arrangements existed that satisfied section s29(5);

d. the AO was a designated person for the purposes of s29;

e. the grant of the authorisation was not in breach of any restrictions imposed by virtue of section 29(7)(a) or 30(3);

f. any other conditions provided for by any Order were satisfied; and

g. there remain reasonable grounds for believing that the necessary and proportionate tests are satisfied and that any other requirements provided for by Order are satisfied.

162. Records should be kept as prescribed by the Code of Practice. Where a source wearing or carrying a surveillance device is invited into residential premises or a private vehicle and records activity taking place inside those premises or vehicle, authorisation for use of that covert source should be obtained in the usual way.

163. The source should not use an invitation into residential premises or private vehicle as a means of installing equipment. If equipment is to be used other than in the presence of the covert source, an intrusive surveillance authorisation is necessary which cannot be granted by a local authority.

164. Regular reviews of authorisations should be undertaken by the AO to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified. The review should include:

a. the use made of the CHIS during the period authorised;

b. the tasks given to the CHIS;

c. the information obtained from the CHIS;

d. if appropriate to the AO’s remit, the reasons why executive action is not possible at this stage.

165. In each case, unless specified by the Secretary of State or Investigatory Powers Commissioner, the AO should determine how often a review should take place. This should be as frequently as is considered necessary and proportionate, but should not prevent reviews being conducted in response to changing circumstances.

166. In the event that there are any significant and substantive changes to the nature of the operation during the currency of the authorisation, the AO should consider whether it is necessary to apply for a new authorisation.

167. CHIS authorisations can be renewed on more than one occasion if necessary and provided that they continue to meet the criteria for authorisation. Before an authorising officer renews an authorisation, they must be satisfied that a review has been carried out of the use of a CHIS and that the results have been considered.

168. All renewals are subject to authorisation by the Court in the established way.

169. When deciding if the relevant source is authorised as part of the 'same investigation or operation' in calculating the period of total or accrued deployment or cumulative authorisation periods, the following should be considered:

a. common subject or subjects of the investigation or operation;

b. the nature and details of relationships established in previous or corresponding relevant investigations or operations;

c. whether or not the current investigation is a development of or recommencement to previous periods of authorisation, which may include a focus on the same crime group or individuals;

d. previous activity by the relevant source that has a bearing by way of subject, locality, environment or other consistent factors should be considered in calculating the period;

e. the career history of the relevant source.

170. All applications for the renewal of an authorisation should record:

a. whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

b. any significant changes to the information in the initial application;

c. the reasons why it is necessary for the authorisation to continue;

d. the use made of the CHIS in the period since the grant or, as the case may be, latest renewal of the authorisation;

e. the tasks given to the CHIS during that period and the information obtained from the use or conduct of the CHIS; and

f. the results of regular reviews of the use of the CHIS.

171. The AO who granted or renewed the authorisation must cancel it satisfied that the use or conduct of the CHIS no longer satisfies the criteria for authorisation, or that arrangements for the CHIS's case no longer satisfy the requirements described in s29.

172. Where the AO is no longer available, this duty will fall to the person who has taken over the role that AO has been assigned to.

173. Where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and risk assessments should be maintained. The AO will wish to satisfy themselves that all welfare matters are addressed, and should make appropriate comment in their written commentary.

174. An authorisation for a CHIS will cease to have effect at the end of a period of 12 months beginning with the day it took effect. However, an authorisation concerning a juvenile CHIS will cease to have effect after 4 months from the date it took effect.