PROCEDURES AND GUIDANCE

Oversight arrangements for covert surveillance and property interference conducted by public authorities and to the activities of relevant sources

Issued by the Chief Surveillance Commissioner

The Rt Hon Lord Judge

July 2016

IMPORTANT NOTICES

The opinions expressed within the Interpretation Guidance section of this publication are those of the Surveillance Commissioners. The OSC is not a judicial authority. This Guidance simply indicates the way in which the Commissioners would be minded to construe particular statutory provisions. There is no statutory requirement to publish them but they are a response to frequent requests for guidance from public authorities or are matters raised or identified during the inspection process. In the absence of case law, they are the most reliable indicator of likely judicial interpretation. They are the basis upon which inspections will be conducted and performance assessed by the Office of Surveillance Commissioners. Applicants and Authorising Officers should take note of the interpretations when constructing and considering applications and authorisations for the use of covert powers.

This document is to be properly promoted by and made accessible to all members of each public authority subject to the oversight of the Chief Surveillance Commissioner. Authorising Officers ought to have a personal copy.

This document is made publicly available to coincide with the laying of the Chief Surveillance Commissioner's Annual Report to the Prime Minister and Scottish Ministers for the period April 2015 - March 2016 and is available in electronic format from the OSC website – https://osc.independent.gov.uk

Extracts may be reproduced but Notes must be copied in full and without alteration. Any extracts must be attributed as "Note [number] of the OSC's 2016 Procedures & Guidance document" either immediately following the extract or as a footnote or endnote.

This document supersedes in its entirety the previous version issued in December 2014. The Chief Surveillance Commissioner, Surveillance Commissioners and Assistant Surveillance Commissioners – all of whom have held judicial office – will note its contents but may exercise individual discretion if they are presented with facts that justify expression of an alternative view.

POST PUBLICATION AMENDMENTS

Note number	Date amended	Nature of amendment

CONTENTS

PART ONE – PROCEDURES

SECTION ONE – INTRODUCTION

GENERAL

1. This document explains the role of the Office of Surveillance Commissioners and how the Commissioners carry out their statutory functions. It also sets out the requirements of the Chief Surveillance Commissioner with regard to the notification of authorisations for property interference, intrusive surveillance and for the activities of "relevant sources" (undercover officers). It takes account of the implementation of The Police Act 1997 ("PA97"), The Regulation of Investigatory Powers Act 2000 ("RIPA"), The Regulation of Investigatory Powers (Scotland) Act 2000 ("RIP(S)A") and amending legislation. It replaces all previous versions of the Procedures and Guidance.

2. For ease of reference, the terms "he" and "his" are used throughout this document.

ROLE OF THE OFFICE OF SURVEILLANCE COMMISSIONERS

3. The OSC is a non departmental public body (NDPB) which was established to oversee the authorisation and use of covert tactics by statutorily empowered public authorities. The work of the OSC is led by the Chief Surveillance Commissioner. He reports directly to the Prime Minister and Scottish Ministers and is supported by Ordinary Surveillance Commissioners, Assistant Surveillance Commissioners, Surveillance Inspectors and a Secretariat.

4. The Commissioners are appointed under Part III of PA97 and RIP(S)A to oversee activities carried out under those Acts as well as under Parts II and III of RIPA.

5. The work of the Commissioners is divided into four main categories:

   i. considering notifications of authorisations for property interference when they are granted, renewed or cancelled
   ii. deciding whether to grant or withhold approval for certain operations under PA97 and under RIPA/RIP(S)A before they take place
   iii. considering notifications of, and (in long term authorisations) deciding whether to grant approval for, the use and conduct of undercover officers
   iv. oversight of the use of powers conferred by the Acts relating to encryption keys.

6. Even if a Commissioner's prior approval is required before an authorisation becomes effective, the responsibility for authorising an activity always remains with the Authorising Officer within the relevant law enforcement agency. It is the responsibility of each Authorising Officer to ensure that any necessary approval is obtained from the Commissioners.

Disclosure of inspection reports

7. Paragraph 9.7 of the Home Office CHIS Code of Practice provides that reports made by the Commissioners concerning the inspection of public authorities and their exercise and performance of powers under RIPA Part II may be made available to the Home Office. Paragraph 9.8 provides that public authorities may publish their inspection reports, in full or in summary, subject to the approval of the OSC at least 10 working days prior to intended publication. These provisions were not made at the request of the Chief Surveillance Commissioner. He does not divulge the content of inspection reports to anyone other than the Chief Officer of the public authority inspected.

8. It is the Chief Officer's prerogative to release the inspection report of his authority in full or in part. If he chooses to do so, he must balance the need for transparency with the need to retain operational security of sensitive tactics and personnel employed by his own authority and by other public authorities in accordance with the Freedom of Information Act. The OSC does not have the capacity to provide approval of disclosure and does not require prior notification of intent to release reports.

How to contact the OSC

9. Any queries on interpretational issues or operating practices should be directed to the appropriate regional office in the first instance. If necessary, queries can be referred to the Secretary of the OSC. Authorisations for England, Wales and Scotland will be processed by the central office and those for Northern Ireland by the Belfast office.

10. Section 2 of this guidance sets out the procedures to be adopted by law enforcement agencies in notifying Commissioners of authorisations and requesting prior approval where appropriate. These procedures only cover the requirements subsequent to authorisation by an Authorising Officer. Procedures prior to this remain the responsibility of the relevant law enforcement agency.

OSC guidance to public authorities

11. The OSC does not give legal advice and any opinion given in a reply to a request to the OSC for guidance does not constitute legal advice and should not be cited as the definitive advice of the OSC. Requests for guidance should only originate from the Senior Responsible Officer of a public authority, or from those working in its covert authorities bureau (or the equivalent RIPA/RIP(S)A monitoring officer or coordinator in local authorities).

12. Guidance may be given, when appropriate, in response to a request from one of the above officers. Such guidance will usually be drafted by the Assistant Surveillance Commissioners and at their discretion. It may not accord with a later opinion of the Commissioners or of the Courts. As for views expressed by Surveillance Inspectors or Assistant Surveillance Commissioners during the course of an inspection, or by Surveillance Commissioners, it is unwise to seek to extrapolate guidance provided in one context to all others. Each case should always be considered on its individual merits. Only the courts can decide what the law is and the trial judge will be the final arbiter as to the admissibility of evidence.

SECTION TWO – CASES REQUIRING NOTIFICATION OR PRIOR APPROVAL

GENERAL

13. Most authorisations, applications for prior approval, renewals and cancellations will be sent to OSC offices by BRENT fax or through CLUSTER. However, there will be occasions outside normal working hours when the Authorising Officer or his staff need to contact the Commissioners directly. This will apply when a Commissioner's prior approval is required for operations that need to start outside office hours. It also applies to cases where the prior approval of a Commissioner would normally be required but where, because of the urgency of the case, prior approval has not been sought or obtained (but see Note 26 below). The OSC will therefore supply force authority bureaux with a rota showing the Duty Commissioners and how they can be contacted.

14. OSC working hours are 9am – 5pm Monday to Friday except for Public Holidays. Advance notice will be given to law enforcement agencies of any extended periods when the office will be unmanned (Christmas and Easter).

PROPERTY INTERFERENCE AND INTRUSIVE SURVEILLANCE OPERATIONS

TIMESCALES

15. All authorisations, renewals and cancellations should be notified to the OSC within four working hours of being given. Renewals should be submitted to the OSC before the existing authorisation expires. If there are any problems in meeting these targets, the OSC should be notified and the reasons explained. If the Authorising Officer is unable to sign the document in time, it should still be sent to meet these deadlines and a signed document sent at the earliest opportunity thereafter.

16. Law enforcement agencies are reminded that, except in urgent cases, requests for prior approval should be sent to the OSC London or Belfast office at least 16 working hours before the surveillance is due to start. Some forces are not following this guidance and are allowing no more than a few hours for Commissioners to consider the papers.

17. For ease of reference, the Chief Surveillance Commissioner's requirements for each type of authorisation are set out below.

NOTIFICATION OF PROPERTY INTERFERENCE AUTHORISATIONS

18. In most cases an authorisation for property interference is notified to a Commissioner for his scrutiny after it has been given, but it is effective from the time of signature by the Senior Authorising Officer. This does not apply to a renewal which, if applied for before the existing authorisation expires, takes effect on expiry.

19. Use the BRENT fax to send the authorisation and all supporting documentation to the appropriate office of the OSC within four working hours of the authorisation being granted.

PRIOR APPROVALS IN INTRUSIVE SURVEILLANCE AND PROPERTY INTERFERENCE CASES

20. In most intrusive surveillance cases and in certain property interference cases, referred to as “prior approval cases”, an authorisation will not take effect until a Commissioner has approved it and the Authorising Officer has been notified in accordance with the legislation. The property interference cases in which prior approval is required are cases where the person giving the authorisation believes that:

    a. any of the property specified in the authorisation is

        i. used wholly or mainly as a dwelling or as a bedroom in a hotel or
        ii. constitutes office premises; OR

    b. the action authorised is likely to result in any person acquiring knowledge of

        i. matters subject to legal privilege
        ii. confidential personal information (of the limited character specified in section 99 of PA97), or
        iii. confidential journalistic material
        iv. confidential constituency information.

Prior approval cases in working hours

21. Use the BRENT fax to send the authorisation and all supporting documentation to the appropriate office of the OSC within four hours of the authorisation being granted, and unless the matter is urgent, at least 16 working hours before the approval is needed.

Prior approval cases outside working hours

22. Contact the Duty Commissioner on the number shown on the duty rota to tell him that the authorisation has been granted and when his approval is likely to be required. He will tell you how and when the papers can be submitted to him.

23. If you have problems contacting the Duty Commissioner for your area of the UK you should contact a Commissioner who is on duty for one of the other areas.

24. If possible, contact a Commissioner as soon as you know that his approval is likely to be needed so that there are no avoidable delays once the authorisation is ready for his consideration.

Renewals of prior approvals

25. Use the BRENT fax to send the authorisation and all supporting documentation to the appropriate office of the OSC within four working hours of the authorisation being renewed and at least 16 working hours before the current authorisation is due to expire. This allows time for the Commissioner to give his approval so that the renewal can become effective before the initial authorisation expires. In default, a fresh application will be required.

Urgent cases where there is not enough time to seek prior approval

26. When the urgency provisions of section 95(1) and 97(3) of PA97 are used and when there is insufficient time to apply for approval (in a case where approval would otherwise be required) an oral authorisation can be granted. The need for prior approval is then dispensed with.

27. Outside working hours contact the Duty Commissioner as soon as practicable after the authorisation is granted (but not between 11pm and 7.30am) and tell him what has been authorised and the grounds for believing that the case was one of urgency. The papers should be sent to the Commissioner (care of OSC) as soon as practicable.

Notifications and renewals of notifications

28. Use the BRENT fax to send the authorisation and all supporting documentation to the appropriate office of the OSC within four working hours of the authorisation being granted or renewed.

Urgent oral authorisations

29. During working hours, use the BRENT fax to send the oral authorisation forms, signed by the applicant and the Authorising Officer, to the appropriate office of the OSC within four working hours of the authorisation being granted. Otherwise, follow the guidance at paragraph 27. A Commissioner will not expect to be provided with the details of an intelligence case.

30. Where law enforcement agencies use mini urgency booklets, these provide the contemporaneous notes of those involved and are the formal record of the Authorising Officer's considerations and instructions given at the time. Whilst these can be forwarded to the OSC, it is vital that the Surveillance Commissioners can read the content. Where clarity of handwriting, or the problems caused by transmission via facsimile machines, will present problems, the law enforcement agency should resolve this before submission.

31. Whilst the contemporaneously written records of urgent oral authorisations are, by their very nature, shorter documents, this does not absolve the Authorising Officer from setting out clearly the reason(s) why the urgency criteria apply; their considerations of necessity, proportionality and collateral intrusion; and precisely what activity they have authorised.

Retractions

32. The OSC will hold authorisations retracted but will not destroy them until the Authorising Officer has written to explain that it has been cancelled and the reasons for retraction before being seen by a Commissioner.

Cancellations

33. Use the BRENT fax to send the cancellation form to the appropriate OSC office within four working hours of the Authorising Officer cancelling the authorisation. It is vital that the cancellation explains: what time the order to cease activity was given; what interference or surveillance was conducted since the authorisation was granted or renewed; the value of the activity and confirmation that all equipment has been recovered.

34. For directed surveillance and CHIS activity which was likely to obtain legally privileged information, the Commissioner will expect to be informed whether legally privileged material has been obtained and, if so, what steps have been taken to deal with it.

OPERATIONS INVOLVING THE USE OF "RELEVANT SOURCES" (UNDERCOVER OFFICERS)

35. For ease of reference, a "relevant source" (as defined by Statutory Instrument 2013/2788) will be referred to within the remainder of this document as an undercover officer.

NOTIFICATION OF UNDERCOVER OFFICER AUTHORISATIONS

36. An authorisation for an undercover officer is notified to a Commissioner for his scrutiny after it has been given, but it is effective from the time of signature by the Authorising Officer. This does not apply to a renewal which, if applied for before the existing authorisation expires, takes effect on expiry and only once a Surveillance Commissioner has granted prior approval.

37. Use the BRENT fax to send the authorisation and the risk assessment associated with that undercover officer to the London office of the OSC within seven days of the authorisation being granted.

38. This time period is stipulated by Statutory Instrument 2013/2788 and therefore also applies to the notification of any authorisation granted under the urgency arrangements, although it would, in the view of the Surveillance Commissioners, be sensible to seek to provide the notification in faster time if practicable, lest they wish to comment.

39. Any authorisation granted using the urgency procedures should be clearly flagged (the notification form contains a box for this) to draw attention to the fact upon receipt in the OSC London office, and to enable its early submission to a Commissioner.

40. Any renewal of an operative following a period of urgent authorisation should be notified to the OSC, with a clear explanation that this is a renewal of an urgent authorisation (which will already have been notified). Any such renewal, in accordance with Statutory Instrument 2013/2788, will ignore the 72 hour period in calculating the validity of the renewal period.

41. Where an undercover officer has been authorised to supplement the activities of existing operatives during the formal review process, a copy of the review form upon which his individual authorisation is contained should be sent, together with the risk assessment relating to him, and a copy of the original authorisation for the operative(s) whom he is now joining within the wider operation. (See also Note 226)

42. Whilst a Commissioner has no power to quash or refuse the initial authorisation of an undercover officer, he may pass comment on the documentation. This will be returned with the notification and should be brought to the immediate attention of the Authorising Officer.

PRIOR APPROVAL OF THE USE AND CONDUCT OF UNDERCOVER OFFICERS

43. Where the use and conduct of an undercover officer must be renewed as a "long term" authorisation (as defined by section 3 of Statutory Instrument 2013/2788), prior approval must be sought in advance of expiry from a Surveillance Commissioner.

The "nine month" stage

44. Where a "long term" deployment is identified for the renewal process, the law enforcement agency must send a notification of this to the London OSC office (the regionally based office arrangements shall not apply in these cases) as soon as the undercover officer reaches the ninth month of his deployment. The law enforcement agency must use the BRENT fax to send the OSC-issued nine month stage notification form, containing basic details. No supporting documentation is required at this stage.

45. Where an undercover officer is authorised for three months because they may acquire legally privileged material (as per the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010), this will need the prior approval of a Surveillance Commissioner at the initial authorisation, and need to be notified for the renewal stage almost immediately.

46. Following receipt of the "nine month stage" notification form, a Surveillance Inspector will be identified to undertake a detailed inspection of all necessary records relating to that undercover officer's authorisation in order to produce a report for the Surveillance Commissioner in advance of the formal renewal request from the law enforcement agency. This report will also be despatched by BRENT fax from the OSC office for the personal attention of the Senior Authorising Officer within the relevant law enforcement agency who will be responsible for considering the renewal.

47. Unless there are unavoidable reasons, the OSC will aim to despatch this report to the Senior Authorising Officer of the relevant law enforcement agency in time for his consideration of the renewal.

Renewal by the Senior Authorising Officer

48. The Senior Authorising Officer should grant a renewal of a "long term" undercover officer, where this is his decision as opposed to a refusal, at around the eleventh month stage of the extant authorisation (or at the two month stage of deployment in the case of a CHIS managed in accordance with the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010). This will provide sufficient time to enable the Surveillance Commissioner to consider whether to grant prior approval for the renewal (which does not take effect until the Commissioner has done so) and allow time for any further details or clarification to be requested and provided.

49. Following the approval of the Senior Authorising Officer, the law enforcement agency should send by BRENT fax a copy of the renewal application, the renewal authorisation, and the risk assessment associated to the undercover officer, to the London OSC office no later than four weeks in advance of the due renewal date.

Prior approval by the Surveillance Commissioner

50. The Surveillance Commissioner will reach his decision on prior approval and this will be communicated to the law enforcement agency. If prior approval is granted, the renewal becomes effective on the date when the original authorisation would otherwise have expired (just as is the case for intrusive surveillance).

Prior approval cases outside working hours

51. As the new prior approval arrangements for undercover officers only apply to "long term" authorisations, there should be no need for making contact with the Commissioners outside working hours, as these renewals will be planned and staged across a three month period (see Notes 43-50).

Monitoring key dates in the new process

52. It is the responsibility of the law enforcement agency concerned to determine the dates when an undercover officer may need to be renewed under the "long term" authorisation arrangements stipulated by Statutory Instrument 2013/2788. The OSC may identify an oversight, but is not responsible for monitoring or calculating "due dates".

Missed renewals

53. If the need for a prior approval renewal has been overlooked, then the law enforcement agency may need to cancel the undercover officer's use and conduct at the end of the "long term" extant authorisation (if it has not already been exceeded) and seek prompt fresh authorisation under the prior approval arrangements. It should not be assumed that a Surveillance Commissioner will be able, or minded, to deal with any such oversight outwith the usual arrangements detailed above.

54. During the intervening period, the undercover officer should not be deployed. Where circumstances demand that he has contact with subjects, for reasons of safety or to deal with a situation involving risk to life or the serious jeopardy of the operation, then the Senior Authorising Officer should consider whether an urgent authorisation, lasting 72 hours, should be granted.

55. In all cases where a prior approval has been overlooked, the OSC London office must be informed at the earliest opportunity and advised of the remedial action taken.

Cancellations

56. Use the BRENT fax to send the cancellation form and the risk assessment for the undercover officer(s) (or comments of the Authorising Officer upon the matter of risk if the latter has not been specifically produced at the time of cancellation) to the London OSC office within four working hours of the Authorising Officer cancelling the authorisation.

57. For any undercover officer activity which was likely to obtain legally privileged information, the Commissioner will expect to be informed whether legally privileged material has been obtained and, if so, what steps have been taken to deal with it.

NOTIFICATION OF COMMISSIONERS' DECISIONS

58. The Commissioners will seek to return decisions on all notifications of authorisation for property interference and intrusive surveillance within 16 working hours, and decisions on applications for their prior approval within eight working hours. If an Authorising Officer needs an application for prior approval to be considered more quickly, he must make this clear when sending the application to the OSC or Duty Commissioner and they will do their utmost to meet your timescales.

APPEALS AGAINST COMMISSIONERS' DECISIONS

Powers of the Commissioners

59. The Commissioners have the power to quash or cancel any authorisation where they are satisfied that the authorisation criteria were not met at the time the authorisation was given or are no longer met. They can quash authorisations given under the urgency provisions if they are satisfied that, at the time of the grant of the authorisation, there were no reasonable grounds for believing that the case was one of urgency. They also have the power to order the destruction of any material obtained other than that required for pending criminal or civil proceedings.

When appeals can be brought

60. PA97, RIPA, RIP(S)A and Statutory Instrument 2103/2788 all provide for the submission by an Authorising Officer of an appeal to the Chief Surveillance Commissioner against Commissioners' decisions.

61. An Authorising Officer may appeal to the Chief Surveillance Commissioner within a period of seven days against any decision made by a Commissioner to:

    a. refuse to approve an authorisation or its renewal

    b. quash an authorisation or renewal

    c. cancel an authorisation or renewal, or

    d. order the destruction of records when cancelling or quashing an authorisation or renewal (other than those required for pending civil or criminal proceedings).

How to appeal

62. All appeals should be sent in the first instance to the Secretary to the Chief Surveillance Commissioner (by secure BRENT or to OSC, PO Box 29105, London, SW1V 1ZU), who will forward them to the Chief Surveillance Commissioner for his consideration.

63. The Authorising Officer should set out the full reasons for appealing, taking into account the grounds on which the Chief Surveillance Commissioner may allow an appeal as specified in the Acts and Statutory Instrument 2013/2788.

64. The Chief Surveillance Commissioner will give notice of his determination to the Authorising Officer concerned and to the Commissioner who made the initial decision.

65. Where he dismisses an appeal, the Chief Surveillance Commissioner will make a report of his findings to the Prime Minister.

SECURE COMMUNICATION ARRANGEMENTS

66. In view of the sensitivity of the material being handled, it is imperative that all parties observe strict security arrangements. In particular, the following points should be borne in mind:

    a. All telephone calls and fax transmissions to and from the OSC and the Commissioners that involve sensitive material must utilise the BRENT encrypted lines. The generally published telephone lines are not secure. All Commissioners have been provided with mobile telephones to ease contact outside office hours but law enforcement agencies should have in mind that this form of communication is not secure.

    b. When sending protectively marked faxes to the OSC offices or the Commissioners, speak to the OSC or the Commissioner on the BRENT telephone number before sending the fax.

    c. Law enforcement agencies will need to ensure that their faxes are connected to BRENT (via a G3FI interface) through the BRENT data port to enable secure telephone conversations to take place at the same time as a fax is being transmitted.

    d. All law enforcement agencies (even those with e-mail links, as out of hours access to Commissioners may still be required) must have BRENT equipment.

    e. The BRENT fax machines in the Secretariat are not capable of receiving information outside normal office hours, i.e. 9am – 5pm Monday to Friday (bar public and pre-advised seasonal holidays).

PART TWO – INTERPRETATIONAL GUIDANCE

Each activity should be considered on its merits

67. It is unacceptable to consider whether an authorisation is required based on the description of the surveillance. Test purchase operations conducted by law enforcement agencies (e.g. in drugs operations) are significantly different from those normally conducted by local authorities (e.g. by Trading Standards). “Drive-by” surveillance may or may not require an authorisation depending on the circumstances.

68. The application of the legal principles of covert surveillance to particular facts is, ultimately, a matter of judgment: the extent to which judgment can be prescribed is limited; there cannot be a one-size-fits-all catalogue of principles, and it would be misleading if Authorising Officers, in particular, were to believe that such a chimera exists.

69. A common error when considering whether authorisation is required is to restrict contemplation to the type of tactic rather than the specific facts of the activity. It is unwise to approach RIPA or RIP(S)A from the perspective of labels.

The effect of section 80 RIPA and section 30 RIP(S)A

70. Part I of RIPA makes unauthorised interception unlawful. In contrast, Part II makes authorised surveillance lawful but does not make unauthorised surveillance unlawful. Whilst not an obligation there is an expectation that Part II covert surveillance is authorised. Section 80 RIPA and section 30 RIP(S)A help a trial judge in exercising his discretion regarding the admissibility of evidence and the impact of the way that evidence was obtained on the fairness of a trial. It is inappropriate to cite these sections as justification for a decision not to authorise. It is unwise for a public authority to rely on them as protection from liability if it chooses not to authorise covert surveillance. It is one of the functions of the Office of Surveillance Commissioners to prevent abuse of discretionary powers.

The roles of the applicant and the Authorising Officer are different

71. The role of the applicant is to present the facts of the application for covert surveillance: the crime to be investigated; the reason why it is proposed to conduct the investigation covertly; what covert tactics are requested and why; whom the covert surveillance will be focused on; who else may be affected by it and how it is intended to conduct covert surveillance. To assist the Authorising Officer’s assessment of proportionality, the applicant should provide facts and evidence but it is not the role of the applicant to establish that it is necessary and proportionate; that is the statutory responsibility of the Authorising Officer.

Necessity

72. The Authorising Officer must be satisfied that the use of covert surveillance is necessary for one of the purposes specified in section 28(3) of RIPA and section 29(3) of RIP(S)A. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether serious crime criteria are met. Often missed is an explanation of why it is necessary to use the covert techniques requested.

Proportionality

73. Proportionality is a key concept of RIPA and RIP(S)A. It is often poorly articulated. An authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

74. A potential model answer would make clear that the following elements of proportionality had been fully considered:

74.1 balancing the size and scope of the operation against the gravity and extent of the perceived mischief

74.2 explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others

74.3 that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and

74.4 providing evidence of other methods considered and why they were not implemented.

"I am satisfied" and "I believe"

75. The Authorising Officer should set out, in his own words, why he is satisfied (RIP(S)A) or why he believes (RIPA) the activity is necessary and proportionate. A bare assertion is insufficient.

An Authorising Officer must demonstrate his satisfaction with the intelligence on which an application is made

76. To assist an Authorising Officer to reach a proper judgment, the value of the data, information or intelligence on which the application has been made should be clear. It is considered best practice for law enforcement agencies to utilise standard evaluation nomenclature which grades both the source and the information. While it is not necessary or desirable in the application to spell out in detail the content of intelligence logs, cross-referencing to these enables an Authorising Officer to check detail. Particular care should be taken when using data or information obtained from open or unevaluated sources such as the Internet or social networks.

77. The law prevents an applicant or Authorising Officer from referring to interception and this presents significant difficulty when covert surveillance is to be based solely on that type of intelligence. Without product derived from other acquisition methods, or an approved summary of the closed material, covert surveillance cannot be authorised.

The impact of UK Statutory Instrument 2010/521 and 2012/1500 (restricting local authority grounds under section 28(3)(b) of RIPA)

78. Local authorities in England and Wales can no longer seek the protection of the Act on the grounds provided by subsections 28(3)(d) and (e) (i.e. in the interests of public safety and for the purpose of protecting public health). In relation to directed surveillance (though not to authorising CHIS), their remaining powers were further limited by Statutory Instrument 2012/1500. To authorise directed surveillance, the Authorising Officer must demonstrate that the proposed activity is necessary for the prevention or detection of a crime which either carries a maximum sentence of at least six months' imprisonment or is an offence relating to the sale of alcohol or tobacco products to minors. (As to the definition of "detecting crime", see RIPA section 81(5).)

All covert activity that is not properly authorised should be reported as soon as it is recognised

79. Activity which should properly be authorised but which isn't should be reported to the Chief Surveillance Commissioner, in writing, as soon as the error is recognised. An initial e-mail alerting the OSC should be followed by a report detailing the circumstances and remedial action submitted by the Chief Officer or Senior Responsible Officer. This does not apply to covert activity which is deliberately not authorised because an Authorising Officer considers that it does not meet the legislative criteria, but allows it to continue. It does include activity which should have been authorised but wasn't or which was conducted outwith the directions provided by an Authorising Officer. All activity which should have been authorised but was not should be recorded and reported to the Inspector(s) at the commencement of an inspection to confirm that any direction provided by the Chief Surveillance Commissioner has been followed.

80. When it is decided to use covert surveillance without the protection of RIPA or RIP(S)A it would be prudent to maintain an auditable record of decisions and actions. Such activity should be regularly reviewed by the Senior Responsible Officer.

The effect of the Policing and Crime Act 2009

81. The Policing and Crime Act 2009 amends section 93 PA97 and sections 29 and 33 of RIPA. It enables law enforcement agencies to enter into written collaborative agreements regarding the provision of support within the operating area of the relevant collaborative units. For a collaboration agreement to take effect, the terms of the agreement must explicitly permit officers of the prescribed rank, grade or office to make applications or authorisations or to have day-to-day responsibility for dealing with a CHIS or to have general oversight of the use made of a CHIS or to have responsibility for maintaining a record of the use made of a CHIS or to be used as a CHIS. The CHIS Code of Practice paragraphs 6.10 to 6.13 provide for the authorised control and handling of a CHIS who benefits more than one authority. The Covert Surveillance and Property Interference Code of Practice paragraphs 3.20 to 3.22 provide for applications and authorisations for directed and intrusive surveillance and property interference where there is a collaboration agreement.

82. If there is no written collaboration agreement, the arrangements provided at paragraphs 7.12 to 7.13 of the Covert Surveillance and Property Interference Code of Practice and paragraph 5.9 of the CHIS Code of Practice must be followed.

Related Authorisations

83. If the action authorised refers to activity under a previous authorisation, the Unique Reference Number (URN) and details of that authorisation (e.g. details of a vehicle which has a VTD fitted) should be given to enable the Commissioner to cross-refer. The Authorising Officer should ensure that what is being granted is not in conflict with previous or other current authorisations. Careful attention must be paid to the relationship between property interference and directed surveillance authorisations to ensure that the subsequent download, interrogation or use of the product from the property interference is clearly spelt out on the associated directed surveillance authorisation. Similarly, authorisations for directed surveillance should only permit the download, interrogation or use of product from interference on the condition that a valid PA97 authorisation exists.

The Authorising Officer must state explicitly what is being authorised

84. Sections 28(4)(a) and 32(5) of RIPA require the Authorising Officer to describe and specify what he is granting. This may or may not be the same as requested by the applicant. For the benefit of those operating under the terms of an authorisation, or any person who may subsequently review or inspect an authorisation, it is essential to produce, with clarity, a description of that which is being authorised (i.e. who, what, where, when and how). The Authorising Officer should as a matter of routine state explicitly and in his own words what is being authorised, and against which subjects, property or location. Mere reference to the terms of the application is inadequate.

Authorisation different from application

85. If an application fails to include an element in the proposed activity which in the opinion of the Authorising Officer should have been included (for example, the return of something to the place from which it is to be taken for some specified activity), or which is subsequently requested orally by the applicant, it may be included in the authorisation; if so, a note should be added explaining why. Conversely, if an Authorising Officer does not authorise all that was requested, a note should be added explaining why. This requirement applies equally to intrusive surveillance, property interference, directed surveillance and CHIS authorisations.

Careful use of words

86. The Authorising Officer must be careful in the use of “or” and “and” in order not to restrict what is intended. For example, do not use “or” when “and” is meant (e.g. “deployment of …. on vehicle A or vehicle B” limits deployment to either vehicle, not both simultaneously or one after the other).

Duration of authorisations and renewals

87. Every authorisation must be for the statutory period, normally three months for surveillance authorisations and twelve months for CHIS authorisations. Thus a surveillance authorisation granted at 14:10 hrs on 9 June will expire at midnight on 8 September. To avoid any risk of ambiguity, this should be expressed as 23:59 hrs on 8 September. If that authorisation is subsequently renewed for a further statutory period, then as with a motor insurance policy, the renewal will begin, using the preceding example, at 00:00 hrs on 9 September, expiring at 23:59 hrs on 8 December, with any subsequent renewal starting at 00:00 hrs on 9 December, and so on. Where longstanding electronic systems or adopted processes show the renewals beginning at 23:59 hrs, thus "losing a day" at each subsequent renewal, OSC Inspectors shall not criticise this, nor consider it a breach. Urgent oral authorisations last for 72 hours (though see Note 295 regarding local authorities in England & Wales). Authorisations for juvenile CHIS last for one month, and for those likely to acquire legally privileged material, three months (with a Surveillance Commissioner's prior approval). For all authorisations the time period begins when an authorisation is granted, unless the prior approval of a Commissioner is required, or a magistrate must first approve the activity (under The Protection of Freedoms Act 2012). In the former, the period begins when written notice of the Commissioner's approval is received by the Authorising Officer. In the latter, upon the date and time the authorisation is approved by the magistrate. The fact that the operation to which the authorisation relates is only expected to last for a short time cannot affect the authorisation period. An early review can take care of issues of continuing necessity and proportionality.

Renewals

88. Renewals can only be granted before the expiry of the existing authorisation and take effect from the time of that expiry. This applies equally to renewals requiring a Commissioner's prior approval, provided that the Authorising Officer has received written notice of that approval before that time.

Dates of effectiveness - leaving date boxes blank

89. Because authorisations requiring prior approval will only be effective on receipt by the Authorising Officer of written notice of the Commissioner's approval, the date boxes should be left blank until the decision has been received. If, for any reason, the Authorising Officer does not personally see a Commissioner's prior approval (for example, when a Chief Constable is out of the force area), receipt in the office of the Authorising Officer will suffice, as an indication of the Authorising Officer having received written notice of approval. See paragraph 6.11 of the Covert Surveillance and Property Interference Code of Practice. The Commissioners require forces which adopt this procedure to notify the Authorising Officer, by an effective and auditable means, of any comments by the Commissioner when giving approval.

Dates of effectiveness - renewal information required by the OSC

90. The OSC must be notified of the effective to and from dates when the authorisation is renewed. Where a renewal requires a Commissioner's prior approval, the dates of effectiveness should be accompanied by a note from the Authorising Officer acknowledging that the dates are conditional upon receipt of approval before the expiry of the current authorisation.

The rank of the Authorising Officer should be provided

91. Every authorisation should show the rank of the person giving it. Designated Deputies must identify themselves as such and say why they are giving the authorisation. ACCs who are not Designated Deputies should state when it would next be reasonably practicable for the Authorising Officer or Designated Deputy to consider the application. Where a new Chief Constable or Designated Deputy is appointed, the OSC should be notified as soon as possible.

Renewals involving minor changes

92. Commissioners are content to treat as renewals authorisations where minor changes have occurred, e.g. the removal of a person or a vehicle from the investigation or the addition to the authorisation of previously unknown details such as a vehicle registration or a subject's identity, provided that the terms of the original authorisation allowed for such amendment. Where details in authorisations are amended at renewal, the reason for further identification or removing subjects or vehicles must be given.

Persons, groups, associates, and vehicles

93. Subject to the guidance at Note 99, reviews and renewals should not broaden the scope of the investigation but can reduce its terms. Where other subjects may unexpectedly come under surveillance, and provided it is justified by intelligence, authorisations can anticipate it by using words such as "suspected of", "believed to be" or "this authorisation is intended to include conversations between any and all of the subjects of this investigation, including those whose identities are not yet known but are believed to be involved in the criminality". When the identities of the other criminal associates and vehicle details become known, they should be identified at review and in the renewal authorisation, so long as this is consistent with the terms of the original authorisation. Otherwise, fresh authorisations are required.

94. When an authorisation includes a phrase such as "...other criminal associates..." a review or renewal can only include those associates who are acting in concert with a named subject within the authorisation (a direct associate) and who are believed to be engaged in crime. It does not enable "associates of associates" to be included, for whom a fresh authorisation is required.

95. Where a person or a vehicle can be identified they must be. If, for example, a subject drives two known vehicles but has access to others and the property interference or covert surveillance may take place on or in any of the vehicles, the wording of the authorisation must reflect this and the two known vehicles be specified in the authorisation, as well as a suitable formula to allow for deployment on as yet unidentified vehicles.

96. It is acceptable to authorise surveillance or property interference against a group or entity involving more than one individual (for example an organised criminal group where only some identities are known) providing that it is possible to link individuals to the common criminal purpose being investigated. It is essential to make explicit the reasons why it is necessary and proportionate to include persons, vehicles or other details that are unknown at the time of authorisation, but once identified they should be added at review (see Note 100). The Authorising Officer should guide the operational commander by setting contextual parameters for the use of the "link" approach.

97. The Authorising Officer should be updated when it is planned to deploy equipment or surveillance against a freshly identified subject before such deployment is made, to enable him to consider whether this is within the terms of his original authorisation, necessary, proportionate and that any collateral intrusion (or interference) has been taken into account; alternatively, where operational demands make it impracticable for the Authorising Officer to be updated immediately, as soon as reasonably practicable thereafter. This is to ensure that the decision to deploy further devices or surveillance remains with the Authorising Officer and is not delegated to, or assumed by, another, such as the operational commander. Such reviews should be pertinent and can be done outwith the usual formal monthly written review process, provided that the details of the Authorising Officer's decisions are recorded contemporaneously and formally updated at the next due review. Where the terms of an authorisation do not extend to interference to other subjects (criminal associates) or their property then a fresh authorisation, using the urgency provisions if necessary, will need to be sought.

98. It is no longer necessary to notify the OSC in writing of the identification of any vehicle, property or person that could not be identified at the time authorisation was given. However, it is vital that details are recorded at the next review or renewal. It is wise to confirm in writing, at cancellation, the details of all property interfered with and all persons subject to surveillance, where these have been identified.

(See also Note 110)

Directed surveillance tactics and techniques may be amended

99. This note applies to directed surveillance only; existing procedures for new interference with property or new methods of intrusive surveillance remain. To comply with *R v Sutherland* the Authorising Officer should clearly set out what activity and surveillance equipment is authorised in order that those conducting the surveillance are clear on what has been sanctioned at each stage in the authorisation process. It is recognised that it is not always possible, at the outset of an investigation, to foresee how it will progress, but this should not provide a reason for applicants to request a wide number of tactics "just in case" they are later needed. The Authorising Officer may not authorise more than can be justified at the time of their decision and should demonstrate control and a proper understanding of necessity, collateral intrusion and proportionality, relating to each tactic requested. In straightforward cases, an applicant should request only the tactics that are known to be available and intended to be used. In more complex cases, where it is foreseen based on operational experience and assessed intelligence that additional tactics may be required as the investigation develops, additional tactics may be requested by way of review. The Authorising Officer should consider the use made of tactics to date, along with their impact and any product, to ensure that each additional tactic is necessary, whether collateral intrusion can be justified, and whether the cumulative effect of the tactics is proportionate in light of progress. Amendment must be explicit and no tactic may be used prior to it being granted by an Authorising Officer. OSC inspections will place significant emphasis on review and renewal procedures to ensure that Authorising Officers are addressing legal requirements throughout the life of an authorisation.

100. Authorisations against a named subject should indicate when, where, and in what circumstances the surveillance is to be carried out.

What must be specified in authorisations (section 32(5) of RIPA and section 6(5) of RIP(S)A)

101. Intrusive Surveillance authorisations must specify or describe (a) the type of surveillance, (b) the premises or private vehicle, and (c) the investigation or operation. For example, an authorisation for the use of an audio device could be for "the monitoring and recording of conversations taking place between X and Y at Z address in connection with operation W, an investigation into drug trafficking".

Crime other than specified in authorisation

102. Discussion by subjects of crimes other than such as are specified in an authorisation need not be disregarded.

Interference when there is no serious crime

103. Interference of this type cannot have the protection of PA97 but it is not unlawful in itself. It is sometimes necessary and proportionate to interfere with property in order to locate a missing person or where there is a perceived threat to life not in relation to criminal conduct or where it is necessary for training purposes. However, it is capable of giving rise to a breach of privacy (e.g. some missing persons may not wish to be located) and law enforcement agencies should have in place a policy and procedure for the use of specialist equipment in these circumstances which should include an audit of the activity sanctioned. There is no requirement to inform the OSC when equipment is used for these purposes but agencies should bring such instances to the attention of the OSC Inspector during the next inspection.

Absence of Authorising Officer (section 94(1) of PA97, section 34(2) of RIPA and section 12(2) of RIP(S)A)

104. It is unlikely to be regarded as "not reasonably practicable" (within the meaning of sections of the Acts specified above) for an Authorising Officer to consider an application, unless he is too ill to give attention, on annual leave, is absent from his office and his home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine. Pressure of work is not to be regarded as rendering it impracticable for an Authorising Officer to consider an application. Where a deputy for a Force Authorising Officer acts in his stead, this should be on a substantive basis as a Superintendent (or equivalent), and not a temporary or convenient arrangement purely for the duration of the consideration of an authorisation in their absence or to cope with reduced headcount.

105. Where a Designated Deputy gives an authorisation the reason for the absence of the Authorising Officer should be stated.

Authorisations under section 93(3) of PA97: execution by another organisation

106. The absence of a collaboration agreement does not preclude the application seeking authorisation of actions by members of another organisation. This guidance is extended to RIPA and RIP(S)A.

(See also Note 112)

Cancel at the earliest opportunity

107. If, during the currency of an authorisation, the Authorising Officer is satisfied that the authorisation is no longer necessary, he must cancel it. It is a statutory requirement that authorisations are cancelled as soon as they are no longer required. In the case of authorisations for property interference and intrusive surveillance, the Authorising Officer should, within four working hours of signing the cancellation, give notice to a Commissioner (which in practice means the OSC) that he has done so.

108. Where interference with more than one property is authorised on a single authorisation (see Note 161) cancellation of individual items may be effected by way of review. The Authorising Officer should fulfil the requirement set out in Note 110. When the interference with all property has ceased a cancellation should be submitted which clarifies which property was interfered with and the duration of each interference.

109. Authorisations may be cancelled orally. When and by whom this was done should be endorsed on the cancellation form when it is completed, and recorded on the Central Record of authorisations.

(See also Part 1, Note 33)

Cancellation – information required

110. Although paragraph 5.18 of the Covert Surveillance and Property Interference Code of Practice is correct in saying that there is no *requirement* for any further details to be recorded when cancelling a directed surveillance authorisation, the Commissioners consider that it would be sensible to complete the authorisation process in a form similar to other parts of the authorisation where relevant details can be retained together. When cancelling an authorisation, the Authorising Officer should:

110.1 Record the date and times (if at all) that surveillance took place and the order to cease the activity was made.

110.2 The reason for cancellation.

110.3 Ensure that surveillance equipment has been removed and returned.

110.4 Provide directions for the management of the product.

110.5 Ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.

110.6 Record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met).

The use by one authority of another to conduct surveillance for a crime that it has no capability to prosecute

111. RIPA and RIP(S)A deal not with enforcement powers but the acquisition of information; there is no obligation to do something with the information collected. It is acceptable for one authority to use the services of another even if the requesting authority has no power or intent to use the product providing that the surveillance is necessary and proportionate to what it seeks to achieve. CHIS should not be exposed to unnecessary risk to obtain information that is unlikely to be used.

The use of external partners

112. When a person who is not an employee of the public authority is authorised to conduct covert surveillance, he is an agent of the public authority. This applies to private contractors or members of another public authority. It is unwise to assume competence and, where there is doubt, an Authorising Officer should check it and record that he has done so. It is wise, if no collaboration agreement exists, to obtain written acknowledgement that they are an agent of the public authority and will comply with the authorisation. Third parties authorised by a public authority are liable to inspection by the Office of Surveillance Commissioners regarding their conduct in relation to the activity authorised.

Disclosure of techniques

113. A Surveillance Commissioner and an Authorising Officer can only authorise on the basis of what has been provided in writing. Issues of disclosure should not inhibit the proper construction of applications and authorisations but can be dealt with at the appropriate time using existing procedures.

One public authority may not force the terms of an authorisation on another

114. One authority may request another to conduct covert surveillance on its behalf (see Note 106) but it may not force those conducting the surveillance to act in a manner that is counter to their beliefs or where the risk is unacceptable to them. If agreement cannot be reached then the requesting authority will have to find an alternative solution.

Requests to amend data

115. If an overt approach is made to the owner of data to amend data that he holds to prevent the compromise of a covert investigation (for example, amendment to flight manifests or delivery tracking details), property interference authorisation is not necessary. It would be prudent, however, for the request and amendments to be made in an auditable manner so that the data owner is appropriately protected.

The retention of applications with 'wet signatures'

116. The key signature is that of the Authorising Officer on the authorisation. The only way it is possible to establish that the Authorising Officer has applied his own mind to the authorisation is if it is handwritten by him. Typed documents are open to the suggestion that the authorisation is prepared by another and simply signed by the Authorising Officer. If information technology is used to construct applications and authorisations, it must be capable of authenticating the author of each version. In the absence of authentication, hand-written (so-called 'wet') signatures are required to avoid accusation that the authorisation has been altered *ex post facto*. If an Authorising Officer relies on words prepared by another, his signature signifies responsibility for those words. Authorisations with wet signatures may be retained by the Authorising Officer or centrally, the latter being the preferred option. It is always open to a trial judge to require evidence which satisfies him that documents relied on are authentic. All public authorities must be ready to provide the relevant witness where authenticity is open to question.

The meaning of Professional Legal Adviser

117. Legal privilege attaches to communications with a legal adviser (usually involving a contractual relationship). It would not normally apply to a Trade Union representative but would normally apply to a Barrister, Solicitor, Legal Executive or Solicitor's Clerk.

The design of forms

118. The Commissioners will continue to criticise the use of forms which do not require the Authorising Officer to fulfil his or her statutory responsibilities. Forms should enable authors to comply with legislation which requires an Authorising Officer to explain the details required by the legislation (see also Notes 75 and 84). There are benefits to the adoption of a common design, but a public authority may amend forms if it encourages precision. The use of pre-scripted assertions is usually inadequate.

Combined authorisations

119. Although an authorisation combining one or more types of covert activity is within the legislation, such contribution often causes error; for example directed surveillance can only be authorised for three months and a CHIS may only be authorised for 12 months and ensuring synchronised documentation is difficult. It should also be remembered that property interference and intrusive surveillance require separate authorisations because they are made under different Acts. (See also Note 161).

Retention of property

120. The principles of RIPA regarding the retention of property apply equally to PA97 (see Covert Surveillance and Property Interference Code of Practice paragraphs 1.2, 9.4 to 9.6 and 7.33 to 7.34).

The Authorising Officer should fully understand the capability of surveillance equipment

121. In order to give proper consideration to collateral intrusion, and to comply with *R v Sutherland,* the Authorising Officer must fully understand the capabilities and sensitivity levels of technical equipment intended to be used, and where and how it is to be deployed. An application which does not assist the Authorising Officer in this respect should be returned for clarification (see also Note 284).

122. The Commissioners are aware that some specialist equipment extracts automatically more data than can be justified as necessary or proportionate and may give rise to collateral intrusion. The inability of technology to restrict capability should not dictate the terms of an authorisation. If data is obtained that exceeds the parameters of an authorisation, the Authorising Officer should immediately review it and make arrangements for its disposal.

Those required to respond to tasking should see the authorisation

123. Where Technical Surveillance Units or other officers are required to respond to tasking, they should see a copy of the authorisation and of any comments by a Surveillance Commissioner or Authorising Officer. For directed surveillance not involving the installation of devices, it is sufficient for the officer in charge of the surveillance team to see these documents and then to brief the team accordingly while taking care to repeat precisely the form of words used by the Authorising Officer. In the case of CHIS, the handler should not proceed until the authorisation has been seen. In each case there should be acknowledgement in writing (with date and time) that the authorisation has been seen.

Private information - activity in public

124. Section 26(2) RIPA does not differentiate between current and historical surveillance product. Sections 48(2) of RIPA and section 31(2) of RIP(S)A define surveillance as including “monitoring, observing or listening” which all denote present activity; but present monitoring could be of past events or the collation of previously unconnected data. Pending judicial decision on this difficult point the Commissioners’ tentative view is that if there is a systematic trawl through recorded data (sometimes referred to as “data-mining”) of the movements or details of a particular individual with a view to establishing, for example, a lifestyle pattern or relationships, it is processing personal data and therefore capable of being directed surveillance.

125. The checking of CCTV cameras or databases simply to establish events leading to an incident or crime is not usually directed surveillance; nor is general analysis of data by intelligence staff for predictive purposes (e.g. identifying crime hotspots or analysing trends or identifying criminal associations). But research or analysis which is part of focused monitoring or analysis of an individual or group of individuals is capable of being directed surveillance and authorisation may be considered appropriate.

(Covert Surveillance and Property Interference Code of Practice 2.6 refers.)

The "Kinloch" judgment (Kinloch v Her Majesty's Advocate [2012] UKSC 62)

126. It is fundamental to all authorisations that they are granted *before* any activity takes place, and thus, before anyone can tell what will happen or has happened. The whole process of authorising covert activity, including what is said at paragraph 1.14 of the Covert Surveillance and Property Interference Code of Practice, is based upon what <u>may</u> happen in terms of likelihood. Put another way, the need for an authorisation has to be judged at the time of authorisation, not with the benefit of hindsight. This principle is crucial when considering the implications of *Kinloch*, where there had been no authorisation but the Supreme Court knew and gave judgment about what had actually happened.

127. The Supreme Court stressed, in paragraph 18 of its judgment, the Strasbourg jurisprudence that "whether there has been an interference with the right to respect for a person's private life.....will depend in each case on its own facts and circumstances". It is of significance that (1) the Court was not considering whether an authorisation for directed surveillance ought to have been granted, nor addressing issues of collateral intrusion or proportionality; and (2) the Court nowhere said or implied that activity in a public place is, if covertly observed by agents of the state, immune from the need for a directed surveillance authorisation.

Biographical information does not satisfy the private information test on its own

128. Use of the term "biographical information" appears to have resulted from the data protection case of *Durant v Financial Services Authority [2003] EWCA Civ 1746*. The Court of Appeal was construing the Data Protection Act 1998, which gave effect to the EC Directive in relation to the protection of personal data and its holding by data controllers. In construing the meaning of "personal data" in section1(1) of the Act, the Court held that one of the two notions which may be of assistance is "whether the information is biographical in a significant sense, that is going beyond the recording of the protective data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy would not be said to be compromised". It is important to note about this decision that:

128.1 Section 1(1) defines “personal data” by reference to individuals who can be identified from data: it is therefore obvious that “personal data” is a different concept from private information

128.2 It was not concerned with RIPA nor was the Court referred to the Strasbourg decisions in relation to private or family life

128.3 “Private information” in RIPA section 26(10) reflects private life in Article 8. “Private life” has been broadly defined at Strasbourg to include professional and business activities.

129. It is dangerously misleading to seek to apply a court’s tests for construing a term in one statute to the construction of a different term in a different statute, particularly when the statutes have different purposes, as these have. “Biographical information” which identifies a subject may be convenient shorthand for identifying some material which directed surveillance may disclose, but it does not cover, for example, a subject’s relationships with others which are part of private and family life.

130. For example, a tracking device, appropriately authorised, which shows a driver visiting his mistress’s address, his children’s school, his bank or any other premises unconnected with crime is likely to give rise to a breach of Article 8 even though these details may not be “biographical information” as defined in *Durant*: it should therefore be authorised as directed surveillance if there is to be RIPA protection.

Central Record of authorisations

131. Paragraphs 8.1 to 8.4 of RIPA and paragraphs 3.14 and 3.15 of RIP(S)A Covert Surveillance and Property Interference Codes of Practice and paragraphs 7.1 to 7.7 of RIPA and paragraphs 3.13 to 3.16 of RIP(S)A CHIS Codes of Practice, detail the requirements for a centrally retrievable record of all authorisations to be held by each public authority. Some aspects of covert policing are especially sensitive and require strict application of the ‘need to know’ principle (e.g. investigations into suspected police misconduct by a force Professional Standards Department, anti-corruption investigations and Special Branch operations). Authorisations (i.e. the document that provides the detail of the activity and the signature of the Authorising Officer) arising from these sensitive matters may be held in separate systems, away from the general run of authorisations, so long as they are centrally retrievable, are accessible to at least the Head of the Central Authorities Bureau (or equivalent unit), in order to ensure proper quality control, and are made available for examination by the relevant Surveillance Commissioner or OSC Inspector.

132. Full compliance is no mere bureaucratic requirement but will allow the person responsible for the Central Record, at a glance, to exercise effective oversight and quality control. It will enable that person to identify when reviews, renewals and cancellations are due, which Authorising Officer is directly involved in any of the operations which they authorise, and will draw attention to investigations likely to involve confidential information.

133. There should be a single centrally retrievable record, preferably in a tabular or electronic format, which contains the information required by the legislation. This record must include references to all the covert activities authorised by a prescribed officer of the authority. Any specialist units applying the 'need to know' principle may retain their own authorisations but must record the Unique Reference Number and key details of the authorisation on the single Central Record.

134. It is acceptable to have a Central Record for all CHIS activity (other than those authorised by the Security Service) and a separate Central Record for all other types of covert surveillance. It is also prudent to maintain a record of PA97 authorisations for property interference in the same place as the record for intrusive surveillance.

135. Local authorities may wish to have a single Central Record to record all covert activity given the smaller levels of usage. It would be sensible for this to include the details of any magistrates' approval under section 32(A) of RIPA.

136. Police Act 1996 collaboration agreements should make explicit provision for the proper keeping of a Central Record. In principle, the Central Record should be maintained by the force providing the Authorising Officer or the designated lead force. If an authorisation is enacted under the terms of a collaboration agreement it is useful to refer to this on the Central Record of authorisations.

The use of template entries

137. Template forms inevitably lead to, or at least give the appearance of, minimal or no consideration of: (a) the nature and extent of the surveillance proposed and the justification for the use of the devices to be employed; (b) necessity; (c) proportionality; (d) collateral intrusion; and (e) what alternative methods have been considered. Template entries are therefore to be avoided or used with great care.

(See also Notes 67 to 69 and 99)

Overseas Surveillance - Schengen Convention

138. Cross-border surveillance is now regulated under the Schengen Convention. Article 40.1 allows officers from one contracting party who are carrying out surveillance to continue that surveillance in the territory of another party where the latter has authorised the surveillance in response to a request for assistance. There are administrative provisions dealing with how and to whom requests for assistance should be made, and there is also provision for the surveillance to be entrusted to officers of the party in whose territory it is to be carried out. RIPA and RIP(S)A will apply in such a case in the UK.

139. Article 40.2 permits the officers carrying out surveillance in one territory to continue it across the border of another territory, where "for particularly urgent reasons" prior authorisation cannot be requested. This permission is subject to a number of conditions, including the requirement for officers to carry identification, make reports, etc. Those which seem significant are as follows:

    139.1 Article 40.2 requires that the appropriate authority in the territory where the surveillance is being carried out should be notified immediately that the border has been crossed, and that a request for assistance should be submitted immediately, explaining the grounds for crossing the border without prior authorisation.

    139.2 Article 40.2 further requires that the surveillance must cease as soon as the contracting party in whose territory it is being carried out so requests or, where no authorisation is obtained in response to the request mentioned above, five hours after the border was crossed.

    139.3 Article 40.3.c provides that entry into private homes and places not accessible to the public is prohibited.

    139.4 Article 40.3.d provides that the officers carrying out the surveillance may neither challenge nor arrest the person under surveillance.

Surveillance outside the UK (RIPA section 27(3))

140. Although under RIPA section 27(3) conduct may be authorised outside the United Kingdom, the application for such an authorisation calls for the exercise of judgment by the applicant because it could only be relevant in the United Kingdom (see Note 162). In case of doubt it is good practice to apply for an authorisation.

Use by officers of covert surveillance devices to confirm at a later date what has been said or done by another person (section 48(2) of RIPA and section 31(2) of RIP(S)A)

141. In IPT/A1/2013 the IPT decided on 24 July 2013 that the covert making of a "voluntary declared interview" in the course of an investigation or operation is not surveillance within the meaning of Part II RIPA.

Length of applications

142. Applications for covert activity should be concise and should only contain material facts. This applies especially to intelligence cases.

143. The issue is one of balance, the object of OSC observations is not to restrict the information to be provided but to achieve a focus on what is really material and avoid burdening the process with information that is not relevant to the decision which is being made.

144. If it aids clarity and reduces reliance on powers of expression, sketches, annotated maps or photographs may be attached to documentation providing they are properly cross-referenced within the main document. Authorising Officers should sign attached documents and ensure that there is adequate information to collate documents if they separate.

Serious crime (section 93(4) of PA97 and section 81(3) of RIPA)

145. An authorisation for property interference cannot be obtained for an operation that does not concern 'serious crime'. If there is uncertainty about whether or not crime is 'serious', it is good practice to seek an authorisation.

Notification signatures

146. Although it is desirable, in exceptional circumstances it may not be necessary for a written notification to a Commissioner to be signed. The name of the Authorising Officer must always be clearly stated.

Collateral Intrusion

147. When notification of property interference is made to a Commissioner, details of any collateral intrusion (interference with persons who are likely to be affected by the interference) that may result as part of it or from use of any equipment put in place must be made known to the Commissioner at the same time. The matters covered by section 7.18 of the Covert Surveillance and Property Interference Code of Practice must be included in the application.

Renewals for property interference and intrusive surveillance must specify all actions taken

148. Commissioners do not see review forms so it is important that renewals for property interference and intrusive surveillance summarily specify all actions taken and material discovered since the previous authorisation was granted.

Continuing interference (sections 92 and 93(1)(a) of PA97)

149. The continuing presence of a surveillance device placed on any private property, including dwellings, hotel bedrooms and private or hired vehicles, is to be treated as a continuing interference. The wording of PA97 (and RIPA or RIP(S)A)) authorisations for surveillance equipment must cover its continued presence.

150. In the event that surveillance equipment is considered to be *lost*, and if all attempts to locate the equipment have been exhausted, the existing property interference authorisation and any associated authorisation may be cancelled. The Chief Surveillance Commissioner should be informed immediately in writing. Should the equipment's location subsequently be identified, a new property interference authorisation should be granted to enable the removal of the equipment as soon as its location is known and the Chief Surveillance Commissioner informed.

151. In the event that equipment is *irretrievable* a property interference authorisation should remain extant until its recovery is possible and any other surveillance authorisation should be cancelled. In extraordinary circumstances, when recovery is unlikely within a reasonable period, the Chief Surveillance Commissioner should be informed in writing detailing the circumstances and requesting permission to cancel the property interference authorisation. In this circumstance, interference continues but the equipment is not being authorised for the purpose of surveillance. If an opportunity to recover the item appears, a new property interference authorisation should be granted. As soon as the equipment is recovered the Chief Surveillance Commissioner should be informed in writing.

Property details (paragraphs 7.6 and 7.7 Covert Surveillance and Property Interference Code of Practice)

152. Interference is "properly authorised" when all property that may be interfered with is identified. It is important that any entry to surrounding property needed to achieve the objective is defined as clearly and as narrowly as possible. A Commissioner will not regard anything that is not specifically mentioned in the authorisation as being authorised.

153. When describing land to be entered, care should be taken to provide Commissioners with sufficient detail to permit the land to be clearly identified (e.g. O.S. grid references with plans showing them and the relevant land).

The effect of section 48(3)(c) of RIPA

154. Surveillance is defined to exclude the product from the interference with property. Searching a vehicle or baggage or placing a device in or on property is interference with it but it is not itself surveillance. There is a difference between activity which a trial judge may consider *"de minimis"* and continuing interference which may provide a profile over time. The use of product from interference may be surveillance and should be separately authorised.

(See also Note 173)

Specify the interference

155. Property Interference authorisations must specify the interference. For example, a search would be authorised as "entry into X address and the recording or copying of any contents believed to be relevant to the investigation into the murder of Y".

156. Interference relates to the deed and is not confined to the purpose. Therefore, there is an expectation of authorisation when property is interfered with during feasibility studies or reconnaissance.

Property interference outside designated operational areas of responsibility when no written collaboration agreement exists

157. All that can be authorised outside a force area is the maintenance and retrieval of equipment. Entry on private land is not covered. Removal of a tracking device to replace its batteries or redeployment of identical equipment amounts to maintenance of the equipment, rather than replacement, and so can take place outside the Authorising Officer's force area, provided that the maintenance was authorised originally. If a property interference authorisation is intended to cover maintenance and retrieval outside the authorisation force area, the Authorising Officer must specify this: see PA97 (as amended) section 93(1)(a). This only extends to entry onto public land to carry out these actions. If entry onto private land outside the Authorising Officer's force area is required, the Authorising Officer of the force area within whose area the land lies must give the authorisation.

158. Any other interference with property or any entry on to private land cannot be authorised outside the force's own area. Any such authorisation has to be sought from the Authorising Officer of the area concerned. Authorisations from outside forces, in particular when property interference is sought, should be accompanied by the supporting directed surveillance authorisation, technical feasibility reports and a comprehensive map indicating where deployment is to take place.

The use of tracking devices

159. Attaching or placing a tracking device onto, or remotely obtaining information about the location of, property without the consent of the owner and when the property is not owned by the investigating authority is interference with property. The usual need to relate the location data obtained by the device to other information causes a potential and foreseeable invasion of privacy even if the location data is historical. In these circumstances it is necessary to obtain a property interference authorisation (to interfere with the property) and usually a directed surveillance authorisation (to make effective use of the product).

Tracking devices and surveillance equipment within public authority vehicles

160. Placing tracking devices or surveillance equipment in or on vehicles owned by the public authority entails no property interference by the authority. The use of a tracking or recording device is unlikely to be regarded as covert if the staff using the vehicle or device are appropriately notified that they are in place for the purpose of recording movements or for safety but may also be used for evidential purposes should the need arise. If equipment is issued to a member of the public authority and used for a purpose not notified to the vehicle occupants this use is covert and an appropriate authorisation should be sought. If a device is installed to covertly monitor, record, observe, or listen to other occupants an authorisation for directed surveillance is required.

Separate authorisations for each property interfered with

161. Separate authorisations are normally required for each property entered or interfered with in order to ensure that full consideration is given to whether each interference is warranted. The only exceptions are:

161.1 where all the properties concerned are owned by the main subject under investigation and it makes administrative sense to combine them. This may cover searches of rubbish at more than one address, if the main subject frequently moves home, or entry on property in order to carry out a feasibility study and subsequently or at the same time deploy technical equipment. However it is not good practice to combine authorisations where part may require cancellation whilst part continues to be needed. Thus a private dwelling and a vehicle, even if belonging to the same person, would require separate authorisations.

161.2 where a subject has access to more than one vehicle, in which case the application can cover as many vehicles as is necessary, if such a wide authorisation is shown to be needed. Such authorisations will normally only cover one subject unless more than one subject uses the same vehicles. All vehicles must be identified whenever it is possible to do so.

161.3 where an operation requires entry on or interference with more than one property in order to achieve the main objective, for example when officers need to cross various pieces of land to reach the property they wish to enter or interfere with, or where there is a need to enter private land to attach a tracking device.

161.4 where a subject is expected to book into one of two or more hotel rooms or two subjects are likely to book into different rooms in the same hotel.

161.5 where persons are suspected of joint involvement in a criminal enterprise.

(See also Note 119)

Overseas surveillance - subject nationality

162. An authorisation under RIPA is required whenever surveillance is carried out overseas by law enforcement agencies either directly or by others on their behalf. But where a subject is neither a UK national nor likely to be the subject of criminal proceedings in this country, and the conduct under investigation would neither affect a UK national nor give rise to material likely to be used in evidence before a UK court, such authorisation is not required.

Overseas deployment of VTDs

163. If a vehicle is expected to be travelling through several countries, it is sufficient for the authorisation to state that the deployment has the approval of the host countries without need for an authorisation for each country. If maintenance or retrieval of surveillance equipment whilst the vehicle is overseas is foreseen then the authorisation should enable this action to be taken.

Extra-territorial offences

164. In relation to offences committed abroad, any actions under the provisions of Part III of PA97 may be undertaken in the United Kingdom only where the serious crime, in the prevention or detection of which such surveillance is likely to be of substantial value, consists of conspiracy to commit offences outside the United Kingdom [see sections 5, 6 and 7 of the Criminal Justice (Terrorism and Conspiracy) Act 1998].

165. Section 27(3) of RIPA provides that the conduct which may be authorised under Part II includes conduct outside the UK. A request for authorisation for surveillance in a Convention State would therefore be competent in terms of UK legislation. However, Article 40 of the Schengen Convention clearly restricts surveillance in the territory of any Convention State and Article 40.3.c, in particular, restricts intrusive surveillance. If any request for authorisation for surveillance in such a State which is party to the relevant provisions of the Convention is made, it should make clear how the surveillance is to be carried out consistently with the Convention, and what steps are being taken to request assistance from the State in question.

Urgent prior approval cases

166. A case is to be regarded as one of urgency within the meaning of the statutory provisions where either (a) the time taken to apply for the approval of a Commissioner, or (b) the further delay following at least one unsuccessful attempt to communicate with a Commissioner, or (c) inability to communicate securely with a Commissioner on account of mechanical failure, would in the judgment of the Authorising Officer, be likely to endanger life or jeopardise the operation in connection with which the surveillance is to be undertaken. A decision to give an authorisation under these circumstances must be notified to a Commissioner as soon as practicable after it is taken even if this is outside normal working hours (but not between 11pm and 7.30am).

Urgent oral authorisation (section 43(1)(a) of RIPA, section 19(1)(a) of RIP(S)A and section 95(1) of PA97)

167. For the purposes of sections 43(1)(a) of RIPA, 19(1)(a) of RIP(S)A and 95(1) of PA97, a case is to be regarded as urgent, so as to permit an authorisation to be given orally, if the time taken to apply in writing would, in the judgment of the person giving the authorisation, be likely to endanger life or to jeopardise the operation for which the authorisation is being given.

168. Paragraph 5.9 of the Covert Surveillance and Property Interference Code of Practice extends RIPA to include the requirement for the Authorising Officer as well as the applicant, when using the urgency provisions, to record the details set out in that paragraph. The Covert Human Intelligence Source Code of Practice (paragraphs 5.12 and 5.13) requires less information to be recorded and then only by the applicant. The Commissioners advise that, in addition to the details set out in the codes of practice, the key issues of necessity, proportionality, collateral intrusion and explicitly what has been authorised should be recorded.

169. Both codes require an urgent oral authorisation to be recorded when "reasonably practicable". The Commissioners advise that notes are made contemporaneously. If, at a later stage, the oral authorisation is recorded in another form (e.g. electronically) care should be taken to copy the contemporaneous notes precisely and not refer to the decision in the past tense. The same considerations apply to the notes and formal records completed by the applicant.

What constitutes 'property' and 'interference' (section 92 of PA97): keys, shoes, baggage searches and computer passwords

170. "Property" includes personal property such as keys and mobile phones.

171. If a computer is set up to work with a password, interference with the password requires an authorisation for property interference. An authorisation under Part III RIPA will be necessary if the owner is required to disclose the password.

172. Taking shoes away for prints is interference, unless authorised under another enactment, whereas taking impressions left after a person has trodden on a mat would not be, provided, of course, that access to the mat was lawful.

173. Deliberately holding up other people's baggage in order to avoid the suspicion of the subject as part of the operational plan to search his luggage constitutes interference. The activity may be considered *"de minimis"* by a trial judge but it should be referred to in authorisations.

174. If software is installed in the computers in an internet café with the consent of the owner in order to determine when a known password is entered, an authorisation for property interference is not required, as the persons using the consoles do not have ownership of this property.

Interference (section 97(2)(a) of PA97)

175. Touching or pushing a door or a window, or putting a probe into a lock of a dwelling, office or hotel bedroom constitutes interference with that property and requires a Commissioner's prior approval before being undertaken.

Multiple vehicles used by a subject of surveillance

176. An authorisation may be expressed to permit interference with any vehicle which the subject may use and any vehicle into which the goods targeted may be transhipped. But such a formula should not be used except in relation to vehicles that cannot be further particularised.

Boats

177. Where it is possible that crew members of a boat may change, it is only necessary to name the owner in an authorisation relating to it.

Placing a device in a vessel (section 97(2)(a) of PA97)

178. Where devices are located on parts of a vessel which, arguably, are not used as a dwelling (such as the engine room) the safer course is nevertheless to seek prior approval.

Covert search of residential premises or a private vehicle and of items found therein (section 26(3-5) of RIPA and section 1(3-5) of RIP(S)A)

179. When a covert search of residential premises or a private vehicle is authorised under PA97 Part III a separate relevant RIPA Part II surveillance authorisation may be required to exploit information that is obtained as a result of that search. A covert search is unlikely to involve monitoring of "anything taking place" at the time of the search and is unlikely to be construed as intrusive surveillance; an authorisation for directed surveillance enabling the examination of items found during the covert search should suffice. Providing an authorisation to interfere with property and an authorisation for directed surveillance enabling the covert examination of items found exists, the location of the examination is irrelevant. A Senior Authorising Officer, when granting property interference, should make clear that he has ensured that a relevant RIPA Part II authorisation enabling the use of the product of the interference was extant at the time the authorisation was granted.

The use of surveillance devices on police property, in places of detention or custody and places of business of a professional legal adviser

180. Covert surveillance carried out in relation to anything taking place on so much of any premises specified in paragraph 4.18 of the Covert Surveillance and Property Interference Code of Practice as is, at any time during the surveillance, used for the purposes of legal consultation, is directed surveillance but shall be processed in the same way as intrusive surveillance (see Statutory Instrument 2010/461) and requires the prior approval of a Surveillance Commissioner. This can only be sought by a law enforcement agency. Surveillance carried out in these places when they are unlikely to be used for the purpose of legal consultation, should be authorised as directed surveillance.

181. Ordinarily a subject should have been interviewed before there is any recourse to listening devices, unless the Authorising Officer believes that further interview(s) will not progress the investigation.

182. When approval is sought for the deployment of surveillance equipment in a room on police premises that has been allocated exclusively to another partner agency or individual for their permanent use it may be expedient to seek a property interference authorisation and a directed surveillance authorisation. In the case of the room being used for legal consultations, the directed surveillance authorisation must be treated as intrusive surveillance and requires the approval of a Commissioner.

Police cells and prison cells (section 97(2)(a) of PA97)

183. No authorisation for property interference is needed for the placing of an audio or video device in a police or prison cell, provided that verifiable consent has been given by the Chief Constable of the appropriate force or by the officer in charge of the cell area.

Items seized under PACE

184. PACE enables overt seizure, examination and retention; it confers lawful possession but does not confer ownership or cover replacement or addition or continued use. However lawful the seizure, examination or retention may be, replacing or adding items or continuing to use the property is an interference with the property of another. PACE does not enable covert surveillance or interference. See also Notes 192-201.

Examination of mobile phones

185. Section 32(9)(b) of PACE, which only applies to arrested persons, allows a constable to retain anything not subject to legal privilege if he has reasonable grounds to believe that it is "evidence of an offence or has been obtained in consequence of the commission of an offence". This provision relates to offences already committed. It cannot extend to anything believed to reveal useful intelligence, the gathering of which will usually be at least part of the purpose of the examination. Section 54(5) of PACE requires that where anything is seized, the person from whom it is seized shall (except in two specified circumstances) be told the reason for the seizure. Ordinarily the purpose will be considerably wider than officers would want the suspect to be told. The examination of any mobile phone will generally be likely to lead to the acquisition of at least some private information. For these reasons, before examining a mobile phone covertly it is prudent to obtain authorisations for both property interference and directed surveillance. The Authorising Officer must be explicit when completing the authorisation regarding what is allowed (e.g. view or extract) and what is to happen in specified circumstances (e.g. when texts or voicemail arrive). Simple references to "examination" or "interrogation" are insufficient. Subject to Note 186 below, authorisations cannot, generally, authorise the opening of stored and accessible voicemail messages or texts <u>whether or not already opened</u> by the recipient. Access to data still in transmission is an interception (see *R v Coulson [2013] EWCA Crim 1026* paragraph 27 which interprets RIPA section 2(7) widely, although CACD were dealing only with voicemail, not texts).

186. RIPA section 1(5)(c) makes lawful access to a stored communication for obtaining information in the exercise of some statutory power, e.g. – property interference under the Police Act 1997 or under PACE 1984. In this particular scenario, no directed surveillance authorisation is needed in addition to the property interference authorisation when downloading [stored] data from a device.

187. The Commissioners are aware that technology is capable of automatically downloading data even though there is no requirement for that data. If it is not possible to control what is downloaded, the use of such equipment should be avoided or the Authorising Officer should restrict the use of product obtained.

Refuse in dustbins (section 92 of PA97)

188. Refuse made available by the occupier of premises for collection by the local authority in dustbins or disposable bags or any other container, whether on private property or in the street, is to be regarded as having been abandoned by the occupier only in favour of the local authority, and it accordingly remains "property" within the meaning of the section.

Items or samples discarded in a public place

189. Where a subject discards an item belonging to him that the police may wish to retrieve in a public place (e.g. for DNA analysis), an authorisation for property interference is not required if the proper inference is that it has been abandoned. However, if a DNA sample is to be taken from property owned by another (for example a glass in a public house) it would be prudent to obtain the consent of the owner of the glass or seek authorisation if such an event could reasonably have been foreseen.

Surveillance devices installed in moveable property

190. Where a surveillance device capable of recording or obtaining private information installed within moveable property (e.g. a parcel or a briefcase) is to be taken into residential premises or a private vehicle, a PA97 authorisation for the "entry" of the device into those premises or the vehicle should be obtained. If the premises are either a dwelling or a hotel bedroom, prior approval of a Commissioner will be required. If the device is to be put into movable property without the property owner's consent, then an authorisation for the installation of the device should also be included.

191. An authorisation for intrusive surveillance need not be obtained just in case a device contained within movable property (e.g. a parcel or a briefcase) ends up in residential premises or a private vehicle. The possibility of a surveillance device, capable of recording or obtaining private information, being introduced into either of these places must be considered at the outset of the operation and a realistic view taken about the need for such authorisation.

Controlled deliveries

192. In the Commissioners' view, in all scenarios whereby an item is to be opened or otherwise interfered with during the course of its onward delivery, without the knowledge of the intended recipient, even if lawfully seized under another power, a property interference authorisation is required. This should include where the contents are extracted for further analysis, and where a substitute item or substance is inserted.

193. Holding or seizing a package during its transit under other statutory powers does not confer ownership (even if the true ownership is unknown or unclear). Suggesting that an illegal commodity can have no "owner" is not an argument accepted by the Commissioners.

194. A property interference authorisation is also required for the insertion of any trigger device, tracking device, and/or recording device.

195. Where such inserted items are likely to be delivered to, or end up within, residential premises or a private vehicle, the property interference authorisation should cater for this (with prior approval for any hotel, office, dwelling or where a recording device may capture confidential information).

196. Where a recording device, light meter or trigger device is likely to end up within residential premises or a private vehicle, then an intrusive surveillance authorisation will also be required.

197. A directed surveillance authorisation is likely to be needed for the later analysis or download of material/recordings/data obtained by means of the initial interference or activation of the device thereafter.

198. In the case of a "dummy package" (whereby a seized package and contents are replaced entirely by a substitute), no property interference authorisation is required in relation to that package, as it is entirely the property of the law enforcement agency in question. However, if any trigger device or such is inserted, then the necessary authorisations should be obtained as per above Notes.

199. If, for the purposes of a controlled delivery, a device is used purely to track an asset in order not to lose "sight" of it, and the data is not going to be used for evidence or to assist in the construction of intelligence, a directed surveillance authorisation may not be required. The relevant legislation is protective: it shall not be unlawful if an authorisation is obtained; it *may* be unlawful if it is not.

200. Every case should be considered on its individual merits. Law enforcement agencies should use their judgment (and seek necessary legal advice as desired) as to whether to seek an authorisation under the Police Act 1997 or RIPA/RIP(S)A.

201. It will be sensible to record the rationale for not authorising any activity, as the Commissioners think that whilst it is unlikely that a trial judge would exclude the evidence in the absence of an authorisation, the law enforcement agency must be ready to show that it had acted in good faith in not having one.

Substantial financial gain (section 93(4)(a) of PA97)

202. "Substantial financial gain" is not defined in either of the Acts. Had Parliament intended this to be a fixed amount for every case it would have said so. In each case it is a matter of judgment by the Authorising Officer whether, taking into account all of the circumstances, the resulting gain is substantial.

203. What is to be considered is belief about resulting gain, not resulting profit. A drug supplier who buys drugs for £500 and sells them for £1,000 gains £1,000 from his supplying. The view may be reasonably taken that a burglar who steals jewellery valued at £1,000 gains £1,000, whether or not he then sells it for £100 or throws it away and whether or not what he throws away is recovered and returned to the loser.

204. In most cases the gain will be that of the offender(s), but gain to others criminally involved is material if it is believed to result from the conduct in question.

Victim communicators

205. When victim communicators or couriers are used in a kidnap or extortion situation, and surveillance equipment is deployed, a RIPA/RIP(S)A authorisation may not be required but, as so much depends on whether or not a crime is in fact being committed and on the scope of the surveillance being proposed, it would, in most cases, be prudent to obtain the appropriate RIPA/RIP(S)A authorisation.

Dwelling (section 97(2)(a) of PA97)and residential premises (section 48(1) of RIPA and section 31(1) of RIP(S)A)

206. PA97 concerns dwellings; RIPA and RIP(S)A concern residential premises. In both cases authorisation for property interference is required and, in the case of dwellings, prior approval of a Commissioner is necessary. The Acts are concerned with use at the time, not permanence.

206.1 Dwelling Prior approval is necessary where any of the property specified is used wholly or mainly as a dwelling (i.e. as a place of abode). Authorisation is therefore necessary for caravans, houseboats, yachts, railway arches, walkers' hides, tents and anywhere else believed to be used as a place to live. An integrated house garage should be regarded as a dwelling. The parts of the premises subject to interference should be specifically identified in the authorisation.

206.2 Residential premises Authorisation for intrusive surveillance is necessary for activity on residential premises involving the presence of an individual or a surveillance device. Hospital wards and police cells are likely to be residential premises but gardens and driveways are not. The parts of the premises subject to interference should be specifically identified and this will determine whether authorisation for intrusive or directed surveillance is appropriate. A lorry with sleeping accommodation should be regarded as residential premises requiring authorisation for intrusive surveillance. Absent any sleeping accommodation, authorisation for directed surveillance will usually suffice for a lorry.

Hotel bedrooms (section 97(2)(a) of PA97)

207. Property Interference authorisation should be given and the prior approval of a Commissioner obtained for any interference with or entry into a hotel bedroom, whether devices are installed before or after allocation, signing the register or entering the room. Even if a device is fitted with the consent of the hotel owner or manager prior to the subject(s) taking occupancy, a property interference authorisation and the prior approval of a Commissioner are still required for the continued presence of the device and any servicing or retrieval of it whilst the room is allocated to the subject.

Interference with leased premises

208. Property leased to a public authority by tenancy agreement does not make the public authority the owner. Without the consent of the owner or a permitting lease, the fabric of such property may only be interfered with (for example by way of installing a listening device or drilling a hole to insert a probe to monitor neighbouring property) after authorisation for property interference and an associated intrusive or directed surveillance authorisation.

Repeat burglary victims and vulnerable pensioners

209. While the consent of the owner to the installation of a surveillance device on his premises avoids the need for a property interference authorisation, the Authorising Officer should consider whether it is likely that the privacy of another person lawfully on the premises may be invaded. Any visitor who is not made aware of it is subject to covert surveillance. This is a technical breach of the visitor's Article 8 rights, although in such circumstances any complaint may be regarded as unlikely.

210. The surveillance is intrusive because it is carried out in relation to things taking place on residential premises: section 26(3)(a). But if the crime apprehended is not "serious", intrusive surveillance cannot be authorised: *cf* section 32(3)(b). On the other hand, the surveillance is not directed, because it is intrusive: section 26(2).

211. The fact that particular conduct may not be authorised under RIPA or RIP(S)A does not necessarily mean that the actions proposed cannot lawfully be undertaken, even though without the protection that an authorisation under the Acts would afford.

212. The Investigatory Powers Tribunal (IPT) has provided clear advice in its judgment in *Addison, Addison & Taylor v Cleveland Police* (IPT/11/129/CHIS; IPT/11/133/CHIS; and IPT/12/72/CHIS) that where no authorisation is capable of being granted in such circumstances, "it will behove a police force to follow a course similar to that adopted here; i.e. a procedure as close as possible to that which would be adopted if an authorisation could be obtained from a Chief Constable [for intrusive surveillance] or other relevant Authorising Officer." The IPT also warned that whilst the conduct in question might be unprotected by an authorisation (as none can be given), that conduct might still be scrutinised by the IPT, and as such, it might not be appropriate to describe any relevant Article 8 breach as "technical".

Binoculars and cameras (section 26(5) of RIPA and section 1(5) of RIP(S)A)

213. If binoculars or cameras are used in relation to anything taking place on any residential premises or in any private vehicle the surveillance can be intrusive even if the use is only fleeting. It will be intrusive "if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle". The quality of the image obtained rather than the duration of the observation is what is determinative.

Stolen vehicles (section 48(1) of RIPA and section 31(1) of RIP(S)A)

214. A stolen vehicle is not a "private vehicle" for purposes of the Acts because a private vehicle is defined by these provisions by reference to use by the owner or person who has the right to use it.

215. When it is intended covertly to track a stolen vehicle, the terms of the legislation can properly be met if regard is had to the following considerations:

215.1 Each authorisation must expressly address proportionality, not only in relation to the interest of the public but also in relation to the owner, so the routine fitting of tracking devices is not permissible.

215.2 Proportionality includes consideration of the particular vehicle and will be affected by such matters as whether the owner has a particular need for the vehicle or its contents, whether the vehicle is likely to be damaged further and whether he has already been paid out by his insurers. (Information as to particular need could be obtained at the time of the original theft: the Commissioners recognise the problem of going back to the owner when fitting the tracking device is being considered.) Unlimited authorisations are unlikely ever to be proportionate.

215.3 Early reviews are likely to be essential.

215.4 The urgency criteria will often be usable.

216. The Commissioners are liable to quash authorisations which are wide in scope and which do not relate to an identified stolen vehicle.

Automated Number Plate Recognition and CCTV lists of interest

217. The 'private life' of a car driver is not interfered with when the registration number of his vehicle is recorded by ANPR while he is travelling on a public road, because the registration plate is a publicly displayed object. It is not adequate to say that recording and storing data capable of identifying the occupants of the car does not require authorisation because they are in a public place: they are, but they are ignorant of the capacity of the camera and the extent to which the data may be retained and used. Some ANPR cameras are now capable of producing clear images of the occupants of a car, as well as the vehicle make and registration number and technology is available which is designed to defeat windshield glare. It is therefore possible to interfere with a person's private life. If the occupant is in a private vehicle such use of ANPR may in consequence constitute intrusive surveillance if data that is recorded for potential later use is capable of identifying him.

218. Monitoring and recording the movements of a specific vehicle or person (persistently or intermittently) over a protracted period or distance, when no action is taken to stop the vehicle or individual when first sighted, is capable of being directed surveillance and an authorisation should be obtained. If the details of persons or vehicles are placed on a list requiring that an investigating officer be notified or a record is made of the location or movements of the person or vehicle, or that vehicle or person is subjected to focused monitoring to build up a picture of the movements of the vehicle or person, an authorisation is expected.

219. It is not the general collection of images of number plates, or coincidental images of occupants, which concerns the Commissioners when interpreting RIPA and RIP(S)A. The reason for placing a vehicle or person on a list of interest, and the action to be taken when they are sighted, are crucial. For example, recording the details of a vehicle related to a traffic offence, where the intention is to stop the vehicle and talk to the driver when sighted, or providing a warning to police that a vehicle is related to offences involving violence are not directed surveillance; both are immediate reactions to events because it could not be foreseen that the vehicle would appear at the given time. However, placing the details of a vehicle or a person on a list because they relate to a criminal investigation or because they have the propensity to commit crime and, when sighted, observing them or placing the time and location on a log for later analysis, is directed surveillance. It follows that it is necessary to have separate lists depending on the action to be taken.

220. The person deciding to place a person or vehicle on a list of interest, where the activity is capable of being construed as covert surveillance, must be competent to make the decision (i.e. must hold the minimum grade, rank or office specified by legislation). If authorised, clear direction is required regarding review, renewal and cancellation (which must include the destruction of data if appropriate and instructions for removal from relevant lists).

Premises set up to monitor traders covertly

221. Premises set up solely for surveillance purposes and not occupied or in current use for residential purposes are not residential premises within section 26(3)(a) of RIPA and surveillance carried out there is therefore not intrusive but may require authorisation for directed surveillance. The position would be otherwise if a variety of devices were deliberately set up in premises which continued to be occupied for residential purposes (sometimes referred to as a "house of horrors"). In some cases a CHIS authorisation may afford protection if the person purporting to be the occupant of the premises establishes or maintains a relationship with a trader and merits consideration depending on the facts.

Authorisation for undercover officers (section 29(4)(b) of RIPA and section 7(5)(b) of RIP(S)A, and Statutory Instrument 2013/2788)

222. With the advent of Statutory Instrument 2013/2788, which came into force on 1st January 2014, the emphasis has been placed firmly on the authorisation of individual undercover operatives instead of the wider operational activity upon which they are deployed.

223. It is the responsibility of law enforcement agencies to ensure that all authorisations and renewals of undercover officers, as defined within Statutory Instrument 2013/2788, and whose renewal beyond twelve months – or three months where there may be access to legally privileged material (article 8(1)(b) of the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010) - now require the prior approval of a Surveillance Commissioner, are brought to the attention of the OSC. Notes 35-52 advise how this is to be done.

224. If a prior approval renewal, or the need for its notification at the nine month stage, is overlooked, there may be limited time left in which to complete the necessary actions, or the operative's valid authorisation period may have already ended. In the latter case, a formal cancellation must be completed and a fresh authorisation (with the prior approval of a Surveillance Commissioner) sought. Where, through oversight, a prior approval renewal is sought from the OSC at very short notice, it shall be at the discretion of the Surveillance Commissioner whether this shall be progressed before the natural expiry date of the valid authorisation. (See also Notes 52-55)

225. More than one undercover officer can be included on a single authorisation document, provided they are individually identified by their unique national index number from the outset. In this case:

225.1 The application and authorisation should clearly address the necessity and proportionality of using multiple operatives, and the collateral intrusion considerations.

225.2 A risk assessment must be completed, pertinent to each individual, which takes into account all the circumstances of the environment in which each is to be deployed and the relevant experience of each operative. This should reflect all other covert activities in which that officer has been, or is contemporaneously, engaged and the level of training the officer has received. This is particularly relevant if the undercover officer comes from a different force, public authority or third party, including from an overseas force. Police collaboration agreements should make arrangement for these details to be made available.

225.3 The Surveillance Commissioners will expect, as a matter of good practice, to see that a risk assessment has been signed or initialled by those holding the section 29(5)(a) and 29(5)(b) roles, and by the Authorising Officer, who should add any relevant comments to the risk assessment form. The Surveillance Commissioners also advise that it is good practice for an Authorising Officer to sign and date each page of the application form to evidence their consideration.

225.4 The Authorising Officer must set out in clear, unequivocal terms, the use and conduct authorised for each individual operative. Particular care is needed where a single authorisation document includes conduct for Foundation and Advanced operatives.

225.5 Where participating conduct is intended for undercover officers, the Surveillance Commissioners are content that if the conduct has been authorised under Part II of RIPA/RIP(S)A it will be lawful for all purposes, as per section 27 of RIPA and section 5 of RIP(S)A. However, the Authorising Officer must stipulate in explicit terms what exactly the undercover officer is authorised to do. Record should also be made (and thus provided) as to what advice has been given by the CPS (PFS in Scotland).

225.6 The records should show clearly which officers hold the roles for the individual undercover officer(s) under section 29(5) of RIPA and section 7(6) of RIP(S)A.

226. An initial authorisation wording can include that, if operationally necessary, additional undercover officers can be authorised. However, each new undercover officer must be authorised formally by way of a review document, or on a separate unique authorisation form, and the considerations of necessity, proportionality, collateral intrusion, and risk must be addressed per operative, and their parameters of engagement made clear. The authorising officer must also record the effective authorisation period applicable to each new undercover operative authorised in this way. (See also Notes 41 and 228)

227. Authorising Officers are responsible for ensuring that the correct authorisation dates for each individual undercover officer are recorded, mindful of the calculation requirements within Statutory Instrument 2013/2788.

228. Reviews of undercover officers' deployments cannot be delegated. Parliament has decreed that authorisations must be by the senior ranks identified within Statutory Instrument 2013/2788, and once authorised, those undercover officers' use and conduct and the duty of care owed to them remain the responsibility of that senior Authorising Officer. In "long term" authorisations, granted prior approval by a Surveillance Commissioner, the ongoing responsibility remains with the Chief Constable or equivalent and similarly, cannot be delegated.

229. If, during their current deployment, an undercover officer is provided with a new personal URN/National Index number, this must be made clear on the documentation and highlighted for the attention of a Surveillance Commissioner where a prior approval renewal is sought. The change in number must also, as soon as the change occurs, be provided to the London OSC office.

The need for an undercover officer authorisation

230. Every case must be considered on its merits, but in relation to the authorisation of the use and conduct of an undercover officer, the Surveillance Commissioners consider this is unlikely to be necessary in cases where there is so fleeting or minimal an engagement with a subject (whether or not identified) that the criteria for a CHIS authorisation are not met. Such examples may include the use of officers as decoys for street robberies; simple exchanges on Internet sites such as eBay to determine the availability of an item and to arrange its purchase (such as in the case of an identified stolen bicycle or counterfeit goods) – see also Note 239; or for simple controlled deliveries to an address, where the intention is to take executive action immediately and the engagement of any subject(s) within the context of the covert delivery is minimal. In every case, the matter should be determined by an Authorising Officer and a written record retained of the rationale for not obtaining a CHIS authorisation.

Use of directed surveillance for a prospective CHIS

231. An assessment of suitability is not usually an investigation of crime under PA97 or any of the other reasons cited in RIPA section 28(3) or 29(3) and section 6(3) of RIP(S)A. Although the use by a police force of covert surveillance to assess the suitability of a person to act as a CHIS cannot usually be authorised under RIPA or RIP(S)A, it should be capable of being justified under Article 8.2 of ECHR.

Pre-authorisation meetings with prospective CHIS

232. An intelligence debrief may not require an authorisation but any tasking to establish or maintain a relationship for a covert purpose or to test reliability may and should be kept under review by an Authorising Officer with appropriate log entries. In principle, it may be better to authorise early and then cancel, if it is later decided not to progress with the CHIS use and conduct, than it is to jeopardise the admissibility of evidence because an authorisation was not obtained. This should not be confused with the assessment of CHIS suitability where no tasking is involved (see also Note 231).

233. "Debriefing" in this sense means obtaining information which it is believed is already known by the person before initial contact. If it is likely that a person, after discussion with a member of a public authority, obtains information as a result of a relationship, which he knows or perceives to be of interest to the public authority, authorisation should be considered.

234. When an individual is rewarded for, or an intelligence report is submitted relating to, information which is used or disclosed in a manner calculated to ensure that the person(s) being reported on are unaware of the use or disclosure in question, the need for authorisation should be seriously considered.

Adult CHIS (including the majority of undercover officers and those authorised to participate in crime) require a full 12 months' authorisation

235. All written authorisations for CHIS, unless they fall for authorisation under the long term authorisation arrangements of Statutory Instrument 2013/2788 or in accordance with the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010, should be of 12 months' duration: *cf.* section 43(3) of RIPA and section 19(1(b)) of RIP(S)A. Reviews, on the other hand, may be conducted at whatever frequency the Authorising Officer deems appropriate (juvenile CHIS require one month authorisation).

Participating CHIS - level of authorisation

236. Notwithstanding the changes brought about in relation to the authorisation of undercover officers, the legislation prescribes the minimum rank or grade for an Authorising Officer granting the use of a CHIS. Some public authorities, in a desire to supervise this type of CHIS more closely, have stipulated a higher rank or grade officer. The legislation enables this but it does not enable an adjustment to the length of an authorisation (Statutory Instrument 2013/2788 excepted) and the Authorising Officer may not delegate all or part of his statutory responsibilities. In other words there can only be one Authorising Officer per CHIS at any time and that person must be responsible for all aspects of use and/or conduct until that specified conduct (i.e. participation) is cancelled.

237. The Commissioners will not criticise an arrangement that retains the rank or grade of an Authorising Officer at the minimum prescribed level but which requires the Authorising Officer to inform a more senior officer of the necessity and proportionality of the use of the CHIS in this way. This will enable the senior officer to consider the corporate risk to the organisation (not the risk to the CHIS or the tactics involved) which will enable the Authorising Officer to make an informed risk assessment. It is imperative that the senior officer does not interfere with the Authorising Officer's statutory responsibilities by providing direction regarding authorisation.

CHIS – Sub-sources and conduits

238. Where the identity of a sub-source is unknown and information said to have been obtained from him/her is passed on to a public authority by a conduit, without the knowledge of the sub-source, the conduit is maintaining a covert relationship with the sub-source and should be treated as a CHIS.

Covert Internet Investigations - e-trading

239. CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage.

CHIS should not be dual authorised

240. The Covert Human Intelligence Source Code of Practice paragraph 2.9 refers to the potential that a single CHIS “may be subject of different use and conduct authorisations obtained by one or more public authorities” and that “such authorisations should not conflict”.

241. A public authority is not entitled to regard a CHIS as its own agent unless it has authorised him or her. For authorisation to be proper it must be given by an organisation with a single system of management. Put another way, there cannot properly be dual authorisation of an individual using more than one Authorising Officer or more than one authorisation for use: the risk of overlap and confusion is obvious and to be avoided. It is possible for an individual to be subject to different conduct authorisations proposed by different public authorities, but a wise Authorising Officer will endeavour to keep the number of simultaneous authorisations to a minimum by way of review (cancelling and combining conduct authorisations when appropriate).

242. The principle of minimising the number of Authorising Officers and authorisations for a single operation or investigation also applies to authorisations to interfere with property, directed surveillance authorisations and section 49 notices.

243. Covert Internet Investigators (now often referred to as undercover officers on line (UCOL)) may establish or maintain a relationship with more than one individual in relation to different investigations. If it is not possible to construct a single authorisation to cover all of the relationships (because the persons with whom relationships are established are not known in advance) it will be necessary to construct for each person with whom a relationship has been established a separate authorisation each of 12 months' duration. It is important that the same Authorising Officer considers each authorisation to ensure that operational conflict and risks do not develop, and to monitor the security and welfare of the CHIS. When appropriate, reviews should be combined to establish whether separate authorisations can be combined into a single authorisation to reduce bureaucracy and error.

Test purchase of sales to juveniles

244. When a young person, pursuant to an arrangement with an officer of a public authority, carries out a test purchase at a shop, he is unlikely to be construed as a CHIS on a single transaction but this would change if the juvenile revisits the same establishment in a way that encourages familiarity. If covert recording equipment is worn by the test purchaser, or an adult is observing the test purchase, it will be desirable to obtain an authorisation for directed surveillance because the ECHR has construed the manner in which a business is run as private information (see also Note 261 and Covert Surveillance and Property Interference Code of Practice paragraphs 2.5 and 2.6) and such authorisation must identify the premises involved. In all cases a prior risk assessment is essential in relation to a young person.

245. When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent “fishing trips”. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been considered or attempted and failed.

246. There is a difference between test purchases to establish whether juveniles are sold goods illegally and a test purchase conducted by a law enforcement officer for the sale of drugs or stolen items. The latter is more likely to require authorisation for the use and conduct of a CHIS. The authorisation always relates to the CHIS relationship and not the operation. All CHIS should be properly risk assessed.

Handlers and Controllers must be from the same investigating authority as the Authorising Officer if no joint working agreement exists.

247. Paragraphs 6.10 to 6.13 of the RIPA CHIS Code of Practice relate to authorisations for the use or conduct of a CHIS whose activities benefit more than a single public authority. In circumstances where a single public authority is the beneficiary of the product obtained from a CHIS, the persons prescribed at section 29(5) of RIPA and section 7(6) of RIP(S)A (usually referred to as the Controller and the Handler) must be from the same investigating authority as the Authorising Officer, unless, in the case of specified law enforcement agencies, an agreement exists under the Police Act 1996 which enables alternative arrangements.

248. The Authorising Officer should carefully consider whether the simple passing of information resulting from a CHIS report is benefiting after the event or whether the benefit is contemplated at the time of authorisation. The Commissioners caution against the term 'beneficiary' being used as a convenience to share resources.

249. If a test purchase officer or undercover officer is accompanied by a cover/welfare officer the latter cannot fulfil the obligations under section 29(5)(a) if there is no written collaboration agreement enabling it.

Joint working – CHIS authorisations

250. The principles of authorisations subject to a collaboration agreement set out in paragraph 3.16 of the RIPA Covert Surveillance and Property Interference Code of Practice should be considered applicable to an authorisation for the use and conduct of a CHIS.

Local Authority CHIS

251. A local authority may prefer to seek the assistance of the police or another public authority to manage its CHIS. In such a case a written protocol between the parties should be produced in order to ensure that an identified CHIS is properly managed (see CHIS Code of Practice 6.12). In the absence of such an agreement the local authority must be capable of fulfilling its statutory responsibilities.

252. Elected members and Senior Responsible Officers (see paragraphs 3.27 and 9.2 of the CHIS Code of Practice) are required to ensure that policies are fit for purpose and that Authorising Officers are competent. An elected member has no need to know the identity of a CHIS nor have access to the product of the use of a CHIS nor know the detail of conduct authorisations. Chief Executives may provide elected members with a copy of OSC inspection reports, redacted if necessary.

253. Some local authorities may not wish to use CHIS and may in practice avoid authorising CHIS. However, all such local authorities should recognise that the occasion may arise when a CHIS appears unexpectedly and has to be authorised and managed. Consequently all local authorities must be equipped with a policy and the awareness training to recognise status drift.

The use of terms other than CHIS

254. The legislation does not envisage a different management regime for different types of CHIS. The term “Tasked Witness” is sometimes used to identify a particular type of CHIS who is willing to testify in court and police officers are variously undercover, test purchase, decoy or covert internet investigators. All types are entitled to all the safeguards afforded a CHIS and the public authority must provide them, including proper considerations for, and completion of, authorisations and risk assessments although some of the factors for consideration, for example when making a risk assessment, may differ as between a CHIS who is an employee of a public authority and one who is a member of the public.

CHIS - remote contact

255. Other than in exceptional and explained circumstances, it is important that regular face-to-face meetings form the primary method for meeting a CHIS rather than remote contact (for example by telephone, text messages or email). The Authorising Officer should question, on review and renewal, why reasonably frequent face-to-face meetings are not being conducted.

Monitoring of CHIS meetings

256. Overt recording of meetings with a CHIS may be made but the product should be properly recorded, cross-referenced and retained. The Authorising Officer should assess and manage the risk of disclosure of audio recordings which may compromise the identity of the CHIS.

Undercover officers - legend construction

257. During the construction of a legend an officer may establish or maintain a relationship with another person who is not the subject of an operation. The nature of that relationship may be for a covert purpose. It will be covert if it is not clear to the other person that the officer is not who he claims to be. The purpose may be to facilitate access to the subject of an operation or to facilitate *bona fide* checks later. If the relationship is for a covert purpose, and the activity relates to a current operation, an authorisation should be obtained. Where the legend is being prepared for possible later use an authorisation may not be necessary. Appropriate arrangements should be in place to manage "status drift".

Repeat voluntary supply of information

258. Some individuals provide information but do not wish to be registered as a CHIS; others repeatedly provide information that has not been sought or where the public authority does not wish to authorise the individual as a CHIS (e.g. because there is evidence of unreliability). If the information being provided is recorded as potentially useful or actionable, there is a potential duty of care to the individual and the onus is on the public authority to manage human sources properly. The legislation is silent regarding consent but sensible procedures should exist to monitor for status drift and to provide the trial judge with a verifiable procedure. Authorising Officers, when deciding whether to grant an authorisation, should take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose as described in paragraphs 2.10 to 2.25 of the CHIS Code of Practice.

Separate CHIS use and conduct authorisations

259. It is the practice of some public authorities to separate the use and conduct authorisations; there is nothing in the legislation to prevent this but it can lead to error. The principle is that there should be a minimum number of authorisations for a CHIS and each authorisation should stand on its own. Conduct authorisations should not conflict and care should be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant reviews, renewals and cancellations are correctly performed.

CHIS interference with property

260. Although it is not encouraged, it is permissible for CHIS to interfere with property (for example, by photocopying documents should an opportunity arise), provided that the terms of the authorisation contemplated this type of conduct. If property interference is foreseen, it would be prudent also to obtain an authorisation for this.

Extent of directed surveillance (section 26 of RIPA and section 1(2) of RIP(S)A)

261. Directed surveillance is covert surveillance that is carried out for the purposes of a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person, whether or not he is a subject of the action. It includes the activity of monitoring, observing, listening and recording by or with the assistance of surveillance equipment. It need not be subject specific. A search for an identified person in a public place will not amount to directed surveillance, unless it includes covert activity that may elicit private information about that person or any other person. Any processing of data (e.g. taking a photograph to put on record) is an invasion of privacy.

Subject or operation specific (section 26(2)(a) of RIPA and section 1(2)(a) of RIP(S)A)

262. Whether a fresh authorisation is required if new subjects emerge depends on the terms of the original authorisation. But in principle these provisions put the emphasis on the operation as being the purpose of the surveillance.

Immediate response (section 26(2) of RIPA and section 1(2)(c) of RIP(S)A)

263. These provisions explain the expression “an immediate response to events or circumstances” by saying “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.” In short, it relates to events or circumstances that occur extemporarily. A response is not to be regarded as “immediate” where the need for an authorisation is neglected until it is too late to apply for it. See also RIPA Covert Surveillance and Property Interference Code of Practice paragraph 2.23.

Crime in progress: private information (section 26(10) of RIPA and section 1(9) of RIP(S)A)

264. As a general principle, if it is clear that a crime is in progress, the offender can have no expectation of privacy and no authorisation for directed surveillance will be required.

265. It is important to differentiate between a crime in progress and a criminal situation which is believed to exist but where evidence may be lacking. In the latter case it would be prudent to obtain an authorisation if time permits.

Describe the operation

266. Authorisations against a named subject should indicate when, where, and in what circumstances the surveillance is to be carried out.

267. Authorisations should specify only the specific covert activities or techniques likely to be required. (See also Note 99)

Pre-emptive directed surveillance authorisations

268. When high grade intelligence is received which enables the production of a plan involving covert surveillance, but where the exact details of the location are not known, it is permissible to prepare an authorisation in order properly to brief those conducting the surveillance. But it must be subject to an immediate review once the missing details are known. It is unwise to act on an incomplete authorisation and this guidance should not be construed as enabling authorisations to be regularly prepared in anticipation of events. The difference between this guidance and use of the urgency provisions is that the urgency provisions may only be used when events could not be anticipated and when there is a threat to life or the operation would be otherwise jeopardised.

Electronic surveillance across the Scottish/English border

269. There is no difference between the method of surveillance (electronic or non-electronic) and the same rules apply to each.

"Drive by" surveillance

270. "Drive by" surveillance may or may not need an authorisation and it is not acceptable to prescribe a minimum number of passes before an authorisation is required.

Use of noise monitoring equipment

271. Measuring levels of noise audible in the complainant's premises is not surveillance because the noise has been inflicted by the perpetrator who has probably forfeited any claim to privacy. Using sensitive equipment to discern speech or other noisy activity not discernible by the unaided ear is covert, likely to obtain private information and may be intrusive surveillance. The Authorising Officer should consider whether the surveillance equipment is capable of measuring volume only or whether it can identify the perpetrators; mindful that the more sensitive the equipment the greater the potential for intrusive surveillance. Where possible, the intention to monitor noise should be notified to the owner and occupier of the premises being monitored. Where notice is not possible or has not been effective, covert monitoring may be considered necessary and proportionate. If monitoring equipment is used as a means also to assess whether a claim is vexatious, any consent provided by the complainant to use monitoring equipment on his premises is vitiated if the full capability of the equipment is not explained.

(See Covert Surveillance and Property Interference Code of Practice 2.30)

CCTV systems - the need for a unified protocol for use

272. It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.

Urgent oral authorisations - essential information to be provided to local authority CCTV managers

273. When an urgent oral authorisation has been issued, the local authority (or any other entity acting on the authorisation) should be provided with the details (including contact information) of the Authorising Officer, the start and expiry date and time and a written summary of what has been authorised (copy of contemporaneous notes taken by the applicant).

Surveillance of persons wearing electronic tags

274. If surveillance against a person wearing an electronic tag is done in a manner not made clear to him, that surveillance is covert and an authorisation should be obtained.

Recording of telephone calls - one party consent

275. Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, a telephone conversation (or other voice data communication such as Voice Over Internet Protocol) may be recorded and authorised as directed surveillance providing that the consent of one of the parties is obtained (see paragraph 2.9 of the RIPA Covert Surveillance and Property Interference Code of Practice). Providing that the original terms of a CHIS authorisation enables it, an additional authorisation for directed surveillance is not required if a CHIS sets out to overhear or record a telephone conversation or other voice data communication (see paragraph 2.30 of the RIPA Covert Surveillance and Property Interference Code of Practice). If there is doubt, it would be prudent to obtain a directed surveillance authorisation. There is no equivalent provision in RIP(S)A.

Closed visits in prison (section 48(7)(b) of RIPA)

276. In prisons closed visits take place in a common area in which booths are set up in such a way as to prevent contact between the inmate and visitor, or in which cubicles are provided in order to afford a limited degree of privacy primarily in relation to other inmates. But whatever form surveillance may take, such a visiting booth or cubicle is not a space being used for residential purposes or otherwise as living accommodation so as to amount to intrusive surveillance. If the surveillance is likely to obtain information subject to legal privilege it is directed surveillance but is authorised using intrusive surveillance processes.

277. Provided that notices are displayed within visiting areas advertising the fact that CCTV is in operation, a directed surveillance authorisation is not needed for visual monitoring of prisoners during open prison visits, as they will be aware that they are under surveillance. But when CCTV is concentrated on a particular visit or visits as part of a pre-planned operation, and private information is likely to be obtained, an authorisation should be applied for.

Crime hotspots (section 26(2) of RIPA and section 1(4) of RIP(S)A)

278. The statutory provisions apply to the obtaining of information about a person whether or not one specifically identified for the purposes of the investigation. It is not restricted to an intention to gain private information because the subsections refer to covert surveillance carried out “in such a manner as is likely to result in the obtaining of private information”.

279. Surveillance of persons while they are actually engaged in crime in a public place is not obtaining information about them which is properly to be regarded as “private”. But surveillance of persons who are not, or who turn out not to be, engaged in crime is much more likely to result in the obtaining of private information about them.

280. An authorisation for Directed Surveillance is required whenever it is believed that there is a real possibility that the manner in which it is proposed to carry out particular surveillance will result in the obtaining of private information about any person, whether or not that person is or becomes a subject of the operation.

(See also Notes 125-126)

Police use of grounds of national security (cf RIPA section 28(3)(a) and 29(3)(a))

281. RIPA enables a Chief Constable (using his Special Branch) to conduct activity on the grounds of national security. The Commissioners acknowledge the Security Service's primacy and would expect a law enforcement agency to offer that Service the opportunity to take the lead (i.e. to authorise). If this offer is rejected, the Chief Constable should not be constrained from investigating using his own resources providing that the grounds of proportionality and necessity are met. If he decides to authorise a CHIS on these grounds, without "concurrence", the CHIS should be managed in accordance with the legislation, codes of practice *and* OSC guidelines.

Surveillance equipment should be under central management

282. All surveillance equipment owned by the public authority should be under central management, since, whatever the object, covert use could be made of most devices. It is considered best practice to cross-reference equipment deployment records with the Unique Reference Number of the relevant authorisation. Where surveillance equipment is shared (e.g. partnership arrangements) there should be auditable processes to prevent unauthorised use of surveillance equipment.

The availability of resources

283. Whilst there may be a public expectation that public authorities will monitor offenders, an Authorising Officer should not grant an activity when he knows there to be insufficient covert surveillance resources to conduct it.

Technical feasibility studies

284. Feasibility studies should be conducted before the application is submitted to the Authorising Officer. Without it the Authorising Officer is unable to know the objectives can be achieved or to accurately assess proportionality or collateral intrusion. It is unacceptable to deny knowledge of technical capability from the Authorising Officer.

Copying property

285. To copy the owner's key would require a PA97 authorisation; to obtain duplicate keys from a manufacturer would not require an authorisation for interference with property but the use of them would require a PA97 authorisation.

Civilian Authorising Officers in law enforcement agencies

286. RIPA and RIP(S)A designate the minimum rank, grade or office of an Authorising Officer; for police force non-urgent authorisations the minimum rank is Superintendent. The omission of the words "or equivalent", which are used for other public authorities, suggest the omission is deliberate. Without amendment to legislation, law enforcement agencies are confined to serving officers. Should legislation be amended to enable a non-serving police officer, it is vital that an Authorising Officer is able to demonstrate competence equivalent to the minimum rank, grade or office specified.

Covert surveillance of cohabiting couples

287. The purpose of surveillance is to investigate a crime and not a criminal. It is usually not possible to be certain of a partner's awareness of a criminal situation and proving cohabitation is sometimes necessary and proportionate. The Commissioners believe that it is appropriate, subject to accurately constructed documents, to authorise surveillance against cohabiting parties. Authorising Officers should confine surveillance of the partner to that which is necessary to prove cohabitation. Surveillance of juveniles or other family members should be avoided.

The Senior Responsible Officer should avoid granting authorisations

288. The role of the Senior Responsible Officer is to oversee the competence of Authorising Officers and the processes in use in his public authority. Whilst legislation does not preclude his use as an Authorising Officer, it is unlikely that he would be regarded as objective if he oversees his own authorisations. For this reason, the Commissioners believe that the Senior Responsible Officer in a law enforcement agency should be of a minimum rank, grade or office equivalent to a Chief Officer (i.e. ACPO/ACPO(S) rank).

Covert surveillance of Social Networking Sites (SNS)

289. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

289.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

289.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).

Technical reconnaissance and feasibility studies

290. If it is likely that during the conduct of a reconnaissance or a feasibility study, property will be interfered with, or private information will be obtained, it should be authorised appropriately.

Updating photographs for intelligence purposes

291. Covertly taking a photograph for the purpose of updating records is capable of being directed surveillance and should be authorised.

Prior approval of a magistrate under section 32A of RIPA (England and Wales only)

292. The Commissioners consider that the best officer to apply to the magistrate for approval of an authorisation of directed surveillance or CHIS is the Authorising Officer, though they recognise that this is not always practicable. Only he can answer questions about his reasoning on necessity, proportionality, collateral intrusion and risk.

293. If the Authorising Officer is not present before the magistrate, any comments made by the magistrate should be promptly reported to him. Such comments might affect the future conduct of the authorised activity, its duration and the regularity of reviews. A record should be made of such comments and of the action taken by the Authorising Officer to incorporate or address them.

294. An authorisation of directed surveillance or CHIS does not take effect until it has been approved and signed by the magistrate. Local authorities should record the dates and times of signature by both the Authorising Officer and the magistrate. Care should be taken to record the expiry date accurately thereafter (see Notes 87 and 135).

295. Local authorities in England and Wales should also bear in mind that the power to make urgent oral authorisations has been removed, because section 43(1)(a) of RIPA no longer applies to authorisations requiring a magistrate's approval. All authorisations, even if urgent, must be made in writing, and local authorities' RIPA policy documents should make this clear.

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Y