Covert Surveillance and Property Interference

Code of Practice

The Scottish Government
Riaghaltas na h-Alba

Covert Surveillance and Property Interference

Code of Practice

Pursuant to Section 24 of the Regulation of Investigatory Powers (Scotland) Act 2000

Contents

1. Introduction 2
2. Directed and intrusive surveillance definitions 6
3. General rules on authorisations 15
4. Legally privileged and confidential information 21
5. Authorisation procedures for directed surveillance 27
6. Authorisation procedures for intrusive surveillance 31
7. Authorisation procedures for property interference 36
8. Keeping of records 42
9. Handling of material and use of material as evidence 44
10. Oversight by Surveillance Commissioners 45
11. Complaints 46
12. Glossary 47

1. Introduction

Definitions

1.1. In this code:

- "RIP(S)A" means the Regulation of Investigatory Powers (Scotland) Act 2000;
- "1997 Act" means the Police Act 1997;
- "RIPA" means the Regulation of Investigatory Powers Act 2000;
- "2010 Order" means the Regulation of Investigatory Powers (Prescription of Offices, etc. and Specification of Public Authorities) (Scotland) Order 2010;
- "2015 Order" means the Regulation of Investigatory Powers (Modification of Authorisation Provisions: Legal Consultations) (Scotland) Order 2015;
- "Police Service" means the Police Service of Scotland;
- "PIRC" means the Police Investigations and Review Commissioner;
- "matters subject to legal privilege" means—

  (a) in relation to authorisations for property interference, matters to which subsection (2), (3) or (4) of section 98 of the 1997 Act applies; or

  (b) in relation to authorisations for covert surveillance—

  (i) communications between a professional legal adviser and the adviser's client; or

  (ii) communications made in connection with or in contemplation of legal proceedings and for the purposes of those proceedings; and
- certain terms are defined in the Glossary at the end of this code.

Background

1.2. This code of practice provides guidance on the use by public authorities of RIP(S)A to authorise covert surveillance that is likely to result in the obtaining of private information about a person. The code also provides guidance on entry on, or interference with, property or with wireless telegraphy by public authorities under Part III of the Police Act 1997.

1.3. This code is issued pursuant to section 24 of RIP(S)A, which stipulates that the Scottish Ministers shall issue one or more codes of practice in relation to the powers and duties in RIP(S)A and Part III of the 1997 Act in so far as relating to the Police Service or the PIRC. This code replaces the previous code of practice issued in 2002.

1.4. This code is publicly available and should be readily accessible by members of any relevant public authority[1] seeking to use RIP(S)A to authorise covert surveillance that is likely to result in the obtaining of private information about a person or Part III of the 1997 Act to authorise entry on, or interference with, property or with wireless telegraphy.

[1] Being one of those listed under section 8(3) of RIP(S)A and specified in orders made by the Scottish Ministers under section 8(1).

1.5. Where covert surveillance activities are unlikely to result in the obtaining of private information about a person, or where there is a separate legal basis for such activities, neither RIP(S)A nor this code need apply.[2]

Effect of code

1.6. RIP(S)A provides that all codes of practice relating to RIP(S)A are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under RIPA, or to one of the Surveillance Commissioners responsible for overseeing the powers conferred by RIP(S)A, it must be taken into account. Public authorities may also be required to justify, with regard to this code, the use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

1.7. Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are not provisions of the code, but are included for guidance only. It is not possible for theoretical examples to replicate the level of detail to be found in real cases. Consequently, authorising officers should avoid allowing superficial similarities with the examples to determine their decisions and should not seek to justify their decisions solely by reference to the examples rather than to the law and the provisions of this code.

Surveillance activity to which this code applies

1.8. RIP(S)A provides for the authorisation of covert surveillance by public authorities where that surveillance is likely to result in the obtaining of private information about a person.

1.9. Surveillance, for the purpose of RIP(S)A, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.[3]

1.10. Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.[4]

1.11. Specifically, covert surveillance may be authorised under RIP(S)A if it is either intrusive or directed:

- intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and

[2] See Chapter 2. It is assumed that intrusive surveillance will always result in the obtaining of private information.
[3] See section 31(2) of RIP(S)A.
[4] As defined in section 1(8)(a) of RIP(S)A.

that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device);[5]

- directed surveillance is covert surveillance that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under RIP(S)A).

1.12. Chapter 2 of this code provides a fuller description of directed and intrusive surveillance, along with definitions of terms, exceptions and examples.

Basis for lawful surveillance activity

1.13. The Human Rights Act 1998 gave effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, while others are qualified, meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when public authorities seek to obtain private information about a person by means of covert surveillance. Article 6 of the ECHR, the right to a fair trial, is also relevant where a prosecution follows the use of covert techniques, particularly where the prosecution seek to protect the use of those techniques through disclosure procedures.

1.14. RIP(S)A provides a statutory framework under which covert surveillance activity can be authorised and conducted compatibly with Article 8. Where directed surveillance would not be likely to result in the obtaining of any private information about a person, no interference with Article 8 rights occurs and an authorisation under RIP(S)A is therefore not appropriate.

1.15. Similarly, an authorisation under RIP(S)A is not required if a public authority has another clear legal basis for conducting covert surveillance likely to result in the obtaining of private information about a person.

1.16. Chapter 2 of this code provides further guidance on what constitutes private information and examples of activity for which authorisations under RIP(S)A are or are not required.

Relevant public authorities

1.17. Only certain public authorities may apply for authorisations under RIP(S)A or the 1997 Act:

- Directed surveillance applications may only be made by those public authorities listed in or added to section 8 of RIP(S)A;

- Intrusive surveillance applications may only be made by those public authorities listed in or added to section 10(1A) of RIP(S)A;

[5] See section 31 of RIP(S)A for full definition of residential premises and private vehicles, and note that the 2015 Order identifies a new category of surveillance to be treated as intrusive surveillance.

- Applications to enter on, or interfere with, property or with wireless telegraphy may only be made (under Part III of the 1997 Act) by those public authorities listed in or added to section 93(5) of the 1997 Act.

Relationship with RIPA

1.18. RIPA is the appropriate legislation for the authorisation of surveillance which:

- will mainly take place outwith Scotland;
- will start outwith Scotland; or
- is for reserved purposes such as national security or economic wellbeing.

1.19. Where the conduct authorised is likely to take place in Scotland, authorisations should be granted under RIP(S)A unless the authorisation is being obtained by certain public authorities (see section 46 of RIPA and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2009; SI No. 3403). RIP(S)A is the appropriate legislation and should be used by Scottish public authorities for all other surveillance (see paragraphs 2.9 – 2.11 in relation to the recording of telephone or other conversations).

1.20. RIPA contains provisions to allow cross border operations. An authorisation under RIP(S)A will allow Scottish public authorities to conduct surveillance anywhere within the UK for a period of up to three weeks at a time (see section 76(2) of RIPA). This three week period will restart each time the border is crossed, provided it remains within the original validity period of the authorisation.

1.21. RIPA authorises surveillance operations in Scotland by public authorities (listed in Schedule 1 to RIPA) other than those specified in section 8(3) of RIP(S)A.

1.22. This code of practice applies in relation to authorisations granted under RIP(S)A. A separate code of practice applies in relation to authorisations granted under RIPA.

International considerations

1.23. Authorisations under RIPA are appropriate for all directed and intrusive surveillance operations in overseas areas under the jurisdiction of the UK, such as UK Embassies, military bases and detention facilities.

1.24. Under the provisions of section 76A of RIPA, as inserted by the Crime (International Co-Operation) Act 2003, foreign surveillance teams may operate in the UK subject to certain conditions. See Chapter 5 (Authorisation procedures for directed surveillance) for detail.

2. Directed and intrusive surveillance definitions

2.1. This chapter provides further guidance on whether covert surveillance activity is directed surveillance or intrusive surveillance, or whether an authorisation for either activity would not be deemed necessary.

Directed surveillance

2.2. Surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIP(S)A to be sought.

2.3. Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person.

Private information

2.4. RIP(S)A states that private information includes any information relating to a person's private or family life[6]. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family[7] and professional or business relationships.

2.5. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis.[8]

Example: Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation.

[6] See section 1(9) of RIP(S)A.
[7] Family should be treated as extending beyond the formal relationships created by marriage or civil partnership.
[8] Note also that a person in police custody will have certain expectations of privacy.

2.6. Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.

Example: Officers of a local authority wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a directed surveillance authorisation should be considered.

2.7. Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate[9].

Example: A surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.

2.8. The use of surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle alone does not necessarily constitute directed surveillance as they do not necessarily provide private information about any individual but sometimes only supply information about the location of that particular device at any one time. However, the use of that information, when coupled with other surveillance activity which may obtain private information, could interfere with Article 8 rights. A directed surveillance authorisation may therefore be appropriate.[10]

Recording of telephone conversations

2.9. The interception of communications sent by public post or by means of public telecommunications systems or private telecommunications is governed by Part I of RIPA. Nothing in this code should be taken as granting dispensation from the requirements of that Part of RIPA.

[9] The fact that a directed surveillance authorisation is available does not mean it is required. There may be other lawful means of obtaining personal data which do not involve directed surveillance.
[10] The use of such devices is also likely to require an authorisation for property interference under the 1997 Act. See Chapter 7.

2.10. Part I of RIPA provides certain exceptions to the rule that interception of telephone conversations must be warranted under that Part. This includes where one party to the communication consents to the interception; that may be regarded as surveillance in accordance with section 48(4) of RIPA provided that there is no interception warrant authorising the interception.

2.11. The recording or monitoring of one or both ends of a telephone conversation by a surveillance device as part of an authorised directed (or intrusive) surveillance operation will not constitute interception under Part I of RIPA provided the process by which the product is obtained does not involve any modification of, or interference with, the telecommunications system or its operation. This will not constitute interception as sound waves obtained from the air are not in the course of transmission by means of a telecommunications system (which, in the case of a telephone conversation, should be taken to begin with the microphone and end with the speaker). Any such product can be treated as having been lawfully obtained.

Example: A property interference authorisation may be used to authorise the installation in a private car of an eavesdropping device with a microphone, together with an intrusive surveillance authorisation to record or monitor speech within that car. If one or both ends of a telephone conversation held in that car are recorded during the course of the operation, this will not constitute unlawful interception provided the device obtains the product from the sound waves in the vehicle and not by interference with, or modification of, any part of the telecommunications system.

Intrusive surveillance

2.12. Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device.

2.13. The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained. In addition, directed surveillance under the ambit of the 2015 Order is to be treated as intrusive surveillance. Accordingly, it is not necessary to consider whether or not intrusive surveillance is likely to result in the obtaining of private information.

Residential premises

2.14. For the purposes of RIP(S)A, residential premises are considered to be so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. This specifically includes hotel or prison accommodation that is so occupied or used.[11] However, common areas (such as hotel dining areas) to which a person has access in connection with their use or occupation of accommodation are specifically excluded.[12]

[11] See section 31(1) of RIP(S)A
[12] See section 31(9) of RIP(S)A

2.15. RIP(S)A further states that the concept of premises should be taken to include any place whatsoever, including any vehicle or moveable structure, whether or not occupied as land.

2.16. Examples of residential premises would therefore include:

- a rented flat currently occupied for residential purposes;
- a prison cell (or police cell serving as temporary prison accommodation);
- a hotel bedroom or suite.

2.17. Examples of premises which would not be regarded as residential would include:

- a communal stairway in a block of flats (unless known to be used as a temporary place of abode by, for example, a homeless person);
- a police cell (unless serving as temporary prison accommodation);
- a prison canteen or police interview room;
- a hotel reception area or dining room;
- the front garden or driveway of premises readily visible to the public;
- residential premises occupied by a public authority for non-residential purposes.

Private vehicles

2.18. A private vehicle is defined in RIP(S)A as any vehicle, including vessels, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This would include, for example, a company car, owned by a leasing company and used for business and pleasure by the employee of a company.[13]

Places for Legal Consultation

2.19. The 2015 Order provides that directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in article 3(2) of the Order as is, at any time during the surveillance, used for the purpose of legal consultations shall be treated for the purposes of RIP(S)A as intrusive surveillance. The premises identified in article 3(2) are:

(a) any premises in which persons who are serving sentences of imprisonment or detention, remanded in custody or remanded or committed for trial or sentence, may be detained;

(b) legalised police cells within the meaning of section 14(1) of the Prisons (Scotland) Act 1989;

(c) any premises in which persons may be detained under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Borders Act 2007;

[13] See section 31(1) and 31(9) of RIP(S)A.

(d) any premises in which persons may be detained under Part VI of the Criminal Procedure (Scotland) Act 1995 or the Mental Health (Care and Treatment) (Scotland) Act 2003;

(e) police stations;

(f) the place of business of any professional legal adviser; and

(g) any premises used for the sittings and business of any court, tribunal or inquiry.

Further considerations

2.20. Intrusive surveillance may take place by means of a person or device located in the residential premises or private vehicle. It may also take place by means of a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as might be expected to be obtained from a device inside.[14]

Example: An observation post outside residential premises which provides a limited view compared to that which would be achievable from within the premises does not constitute intrusive surveillance. However, the use of a zoom lens, for example, which consistently achieves imagery of the same quality as that which would be visible from within the premises, would constitute intrusive surveillance.

2.21. The use of a device for the purpose of providing information about the location of any private vehicle is not considered to be intrusive surveillance.[15] Such use may, however, be authorised as directed surveillance, where the recording or use of the information would amount to the covert monitoring of the movements of the occupant(s) of that vehicle. A property interference authorisation may be appropriate for the covert installation or deployment of the device.

Where authorisation is not required

2.22. Some surveillance activity does not constitute intrusive or directed surveillance for the purposes of RIP(S)A and no directed or intrusive surveillance authorisation can be provided for such activity. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to specified grounds;
- overt use of CCTV and ANPR systems;
- certain other specific situations.

2.23. Each situation is detailed and illustrated below.

[14] See section 1(5) of RIP(S)A.
[15] See section 1(4) of RIP(S)A.

Immediate response

2.24. Covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events would not require a directed surveillance authorisation. RIP(S)A is not intended to prevent public authorities from fulfilling their legislative functions. To this end section 1(2)(c) of RIP(S)A provides that surveillance is not directed surveillance when it is carried out by way of an immediate response to events or circumstances the nature of which is such that it is not reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

Example: An authorisation under RIP(S)A would not be appropriate where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol.

General observation activities

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

Example 1: Plain clothes police officers on patrol to monitor a high street crime hot-spot or prevent and detect shoplifting would not require a directed surveillance authorisation. Their objective is merely to observe a location and, through reactive policing, to identify and arrest offenders committing crime. The activity may be part of a specific investigation but is general observational activity, rather than surveillance of individuals, and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.

Example 2: Local authority officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again this is part of the general duties of public authorities and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.

Example 3: Surveillance officers intend to follow and observe Z covertly as part of a pre-planned operation to determine her suspected involvement in shoplifting. It is proposed to conduct covert surveillance of Z and record her activities as part of the investigation. In this case, private life considerations are likely to arise where there is an expectation of privacy and the covert surveillance is pre-planned and not part of general observational duties or reactive policing. A directed surveillance authorisation should be considered.

Surveillance not relating to specified grounds or core functions

2.26. An authorisation for directed or intrusive surveillance is only appropriate for the purposes of a specific investigation or operation, insofar as that investigation or operation relates to the grounds specified at section 6(3) or 10(2) of RIP(S)A. Covert surveillance for any other general purposes

should be conducted under other legislation, if relevant, and an authorisation under RIP(S)A should not be sought.

2.27. A public authority may only engage RIP(S)A when in performance of its 'core functions'. The 'core functions', as referred to by the Investigatory Powers Tribunal (C v The Police and the Secretary of State for the Home Office - IPT/03/32/H dated 14 November 2006), are the 'specific public functions', undertaken by a particular authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc). The disciplining of an employee is not a 'core function', although related criminal investigations may be. The protection of RIP(S)A may therefore be available in relation to associated criminal investigations so long as the activity is deemed to be necessary and proportionate.

Example: A police officer is suspected by the Police Service of undertaking additional employment in breach of discipline regulations. The Police Service wishes to conduct covert surveillance of the officer outside the police work environment. Such activity, even if it is likely to result in the obtaining of private information, does not constitute directed surveillance for the purposes of RIP(S)A as it does not relate to the discharge of the Police Service's core functions. It relates instead to the carrying out of ordinary functions, such as employment, which are common to all public authorities. Activities of this nature are covered by the Data Protection Act 1998 and employment practices code[16].

Example 2: A police officer claiming compensation for injuries allegedly sustained at work is suspected by the Police Service of fraudulently exaggerating the nature of those injuries. The Police Service wishes to conduct covert surveillance of the officer outside the work environment. Such activity may relate to the discharge of the Police Service's core functions as the Police Service may launch a criminal investigation. The proposed surveillance is likely to result in the obtaining of private information and, as the alleged misconduct amounts to the criminal offence of fraud, a directed surveillance authorisation may be appropriate.

CCTV and ANPR (Automatic Number Plate Recognition) Cameras

2.28. The use of overt CCTV cameras by public authorities does not normally require an authorisation under RIP(S)A. Members of the public will be aware that such systems are in use[17], and their operation is covered by the Data Protection Act 1998 and the CCTV Code of Practice 2008, issued by the Information Commissioner's Office. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an authorisation under RIP(S)A.

2.29. The Protection of Freedoms Act 2012 requires that a Surveillance Camera Code[18] of Practice for England and Wales be published. While this does not extend to Scotland, RIP(S)A authorities may find it useful to take into

[16] For further information see www.ico.org.uk
[17] For example, by virtue of cameras or signage being clearly visible.
[18] http://ico.org.uk/for_the_public/topic_specific_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/cctv-code-of-practice.pdf

consideration when preparing to engage cameras for directed or intrusive surveillance.

Example: Overt surveillance equipment, such as town centre CCTV systems or ANPR, is used to gather information as part of a reactive operation (e.g. to identify individuals who have committed criminal damage after the event). Such use does not amount to covert surveillance as the equipment was overt and not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation.

2.30. However, where overt CCTV or ANPR cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV or ANPR system in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

Example: A local police team receives information that an individual suspected of committing thefts from motor vehicles is planning to commit further thefts in a town centre area. A decision is taken to use the town centre CCTV system to conduct surveillance against that individual such that he remains unaware that there may be any specific interest in him. This targeted, covert use of the overt town centre CCTV system to monitor and/or record that individual's movements should be considered for authorisation as directed surveillance.

Specific situations not requiring authorisation

2.31. The following specific activities also constitute neither directed nor intrusive surveillance:

- the use of a recording device by a covert human intelligence source in respect of whom an appropriate use or conduct authorisation has been granted permitting him to record any information obtained in his presence; [19]
- the recording, whether overt or covert, of an interview with a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a member of a public authority. In such circumstances, whether the recording equipment is overt or covert, the member of the public knows that they are being interviewed by a member of a public authority and that information gleaned through the interview has passed into the possession of the public authority in question[20];
- the covert recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels. In such circumstances the perpetrator would normally be regarded as having forfeited any claim to privacy and an authorisation may not be necessary;

[19] See section 31(3) of RIP(S)A.
[20] http://www.ipt-uk.com/docs/IPT_A1_2013.pdf

- entry on or interference with property or wireless telegraphy under Part III of the 1997 Act (such activity may be conducted in support of surveillance, but is not in itself surveillance).[21]

[21] See section 31(3) of RIP(S)A.

3. General rules on authorisations

Overview

3.1. An authorisation under RIP(S)A will, providing the statutory tests are met, provide a lawful basis for a public authority to carry out covert surveillance activity that is likely to result in the obtaining of private information about a person. Similarly, an authorisation under Part III of the 1997 Act will provide lawful authority for constables or PIRC staff officers to enter on, or interfere with, property or wireless telegraphy.

3.2. Responsibility for granting authorisations varies depending on the nature of the operation and the public authority involved. The relevant public authorities and authorising officers are detailed in the 2010 Order.

Necessity and proportionality

3.3. RIP(S)A and the 1997 Act stipulate that the person granting an authorisation or warrant for directed or intrusive surveillance, or interference with property, must believe that the activities to be authorised are necessary on one or more statutory grounds.[22]

3.4. If the activities are deemed necessary on one or more of the statutory grounds, the person granting the authorisation must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

3.5. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.6. The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

[22] These statutory grounds are laid out in sections 6(3) of RIP(S)A for directed surveillance; section 10(2) of RIP(S)A for intrusive surveillance; and section 93(2) of the 1997 Act for property interference. They are detailed in Chapters 5, 6 and 7 for directed surveillance, intrusive surveillance and interference with property respectively.

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

3.7. It is important therefore that all those involved in undertaking directed or intrusive surveillance activities or interference with property under RIP(S)A or the 1997 Act are fully aware of the extent and limits of the authorisation in question.

Example 1: An individual is suspected of carrying out a series of criminal damage offences at a local shop, after a dispute with the owner. It is suggested that a period of directed surveillance should be conducted against him to record his movements and activities for the purposes of preventing or detecting crime. Although these are legitimate grounds on which directed surveillance may be conducted, it is unlikely that the resulting interference with privacy will be proportionate in the circumstances of the particular case. In particular, the obtaining of private information on the individual's daily routine is unlikely to be necessary or proportionate in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as overt observation of the location in question until such time as a crime may be committed.

Example 2: An individual is suspected of claiming a false address in order to abuse a school admission system operated by his local education authority. The local authority considers it necessary to investigate the individual for the purpose of preventing or detecting crime. Although these could be legitimate grounds for seeking a directed surveillance authorisation, if the individual's actions were capable of constituting a crime, such surveillance is unlikely to be necessary or proportionate to investigate the activity. Instead, it is likely that other less intrusive, and overt, means (such as unscheduled visits to the address in question) could be explored to obtain the required information.

Example 3: An individual is suspected of a relatively minor offence, such as littering, leaving waste out for collection a day early, or permitting dog-fouling in a public place without clearing up afterwards. It is suggested that covert surveillance should be conducted against her to record her movements and activities for the purposes of preventing or detecting crime, or preventing disorder. Although these could be legitimate grounds for seeking a directed surveillance authorisation, if the individual's actions were capable of constituting an offence or disorder, strong consideration should be given to the question of proportionality in the circumstances of this particular case and the nature of the surveillance to be conducted. In particular, the obtaining of private information on the individual's daily routine is unlikely to be necessary or proportionate in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as general observation of the location in question until such time as a crime may be committed. In addition, it is likely that such offences can be tackled using overt techniques.

Collateral intrusion

3.8. Before authorising applications for directed or intrusive surveillance, the authorising officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance or property interference activity (collateral intrusion).

3.9. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

3.10. All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed actions.

3.11. Where it is proposed to conduct surveillance activity or property interference specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such surveillance or property interference activity should be carefully considered against the necessity and proportionality criteria as described above (paragraphs 3.3-3.7).

Example: A law enforcement agency seeks to conduct a covert surveillance operation to establish the whereabouts of N in the interests of preventing a serious crime. It is proposed to conduct directed surveillance against P, who is an associate of N but who is not assessed to be involved in the crime, in order to establish the location of N. In this situation, P will be the subject of the directed surveillance authorisation and the authorising officer should consider the necessity and proportionality of conducting directed surveillance against P, bearing in mind the availability of any other less intrusive means to identify N's whereabouts. It may be the case that directed surveillance of P will also result in obtaining information about P's family, which in this instance would represent collateral intrusion also to be considered by the authorising officer.

Combined authorisations

3.12. A single authorisation may combine:

- any number of authorisations under RIP(S)A;[23]
- an authorisation under RIP(S)A and an authorisation under Part III of the 1997 Act;

3.13. For example, a single authorisation may combine authorisations for directed and intrusive surveillance. However, the provisions applicable for each of the authorisations must be considered separately by the appropriate authorising officer. Thus, a police superintendent could authorise the directed surveillance element but the intrusive surveillance element would need the separate authorisation of the chief constable of the Police Service (or a senior officer designated by the chief constable) and the approval of a Surveillance Commissioner, unless the case is urgent.

[23] see section 19(2) of RIP(S)A.

3.14. The above considerations do not preclude public authorities from obtaining separate authorisations

Collaborative working

3.15. Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should consult the authorising officer within the police area in which the investigation or operation is to take place.

3.16. In cases where one public authority is acting on behalf of another, the tasking authority should normally obtain or provide the authorisation under RIP(S)A. For example, where surveillance is carried out by the Police Service on behalf of a local authority, authorisations would usually be sought by the local authority and granted by the appropriate authorising officer within that authority. Where the operational support of other authorities (in this example, the Police Service) is foreseen, this should be specified in the authorisation. Failure to do so does not mean that other authorisations may not subsequently be used to assist the investigation.

3.17. Where possible, public authorities should seek to avoid duplication of authorisations as part of a single investigation or operation. For example, where two authorities are conducting directed or intrusive surveillance as part of a joint operation, only one authorisation is required. Duplication of authorisations does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on authorities.

3.18. Where an individual or a non-governmental organisation is acting under direction of a public authority then they are acting as an agent of that public authority and any activities they conduct which meet RIP(S)A definitions of directed or intrusive surveillance or the 1997 Act definition of property interference should be considered for authorisation under those Acts.

3.19. Police Service applications for directed or intrusive surveillance and property interference must only be made by a constable of the Police Service .

3.20. Authorisations for intrusive surveillance relating to residential premises, and authorisations for property interference, may only authorise conduct where the premises or property in question are in Scotland.

Reviewing authorisations

3.21. Regular reviews of all authorisations should be undertaken to assess the need for the surveillance or property interference activity to continue. The results of a review should be retained for at least three years (see Chapter 8). Particular attention is drawn to the need to review authorisations

frequently where the surveillance or property interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

3.22. In each case the frequency of reviews should be considered at the outset by the authorising officer. This should be as frequently as is considered necessary and practicable.

3.23. The authorising officer is usually best placed to assess whether the authorisation should continue or whether the criteria on which he based the original decision to grant an authorisation have changed sufficiently to cause the authorisation to be revoked. Support staff can do the necessary research and prepare the review process but the actual review is the responsibility of the original authorising officer and should, as a matter of good practice, be conducted by them or, failing that, by an officer who would be entitled to grant a new authorisation in the same terms.

3.24. Any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in further or greater intrusion into the private life of any person should also be brought to the attention of the authorising officer by means of a review. The authorising officer should consider whether the proposed changes are proportionate (bearing in mind any extra intended intrusion into privacy or collateral intrusion), before approving or rejecting them. Any such changes must be highlighted at the next renewal if the authorisation is to be renewed.

3.25. Where a directed or intrusive surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at a review to include the identity of these individuals. It would be appropriate to convene such a review specifically for this purpose. This process will not require a fresh authorisation, providing the scope of the original authorisation envisaged surveillance of such individuals. Such changes must be highlighted at the next renewal if the authorisation is to be renewed.

Example: A directed surveillance authorisation is obtained by the Police Service to authorise surveillance of "X and his associates" for the purposes of investigating their suspected involvement in a crime. X is seen meeting with A in a café and it is assessed that subsequent surveillance of A will assist the investigation. Surveillance of A may continue (he is an associate of X) but the directed surveillance authorisation should be amended at a review to include "X and his associates, including A".

General best practices

3.26. The following guidelines should be considered as best working practices by all public authorities with regard to all applications for authorisations covered by this code:

- applications should avoid any repetition of information;
- information contained in applications should be limited to that required by the relevant legislation[24];

[24] As laid out in Chapters 5, 6 and 7 of this code.

- where authorisations are granted orally under urgency procedures (see Chapters 5, 6 and 7 on authorisation procedures), a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the applicant and authorising officer as a priority. There is then no requirement subsequently to submit a full written application;
- an application should not require the sanction of any person in a public authority other than the authorising officer;
- where it is foreseen that other agencies will be involved in carrying out the surveillance, these agencies should be detailed in the application;
- authorisations should not generally be sought for activities already authorised following an application by the same or a different public authority.

3.27. Furthermore, it is considered good practice that within every relevant public authority, a senior responsible officer[25] should be responsible for:

- the integrity of the process in place within the public authority to authorise directed and intrusive surveillance and interference with property or wireless telegraphy;
- compliance with RIP(S)A, Part III of the 1997 Act and with this code;
- engagement with the Surveillance Commissioners and Inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Surveillance Commissioner.

3.28. Within local authorities, the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioner. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed.

3.29. In addition, elected members of a local authority should review the authority's use of RIP(S)A and set the policy at least once a year. They should also consider internal reports on use of RIP(S)A on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations. In regard to the matters mentioned in this paragraph, local authorities may wish to consider ensuring that their elected members have undergone sufficient training in order to fulfil these requirements.

[25] The senior responsible officer should be a person holding the office, rank or position of an authorising officer within the relevant public authority.

4. Legally privileged and confidential information

Overview

4.1. RIP(S)A does not provide any special protection for 'confidential information', although the 1997 Act makes special provision for certain categories of confidential information. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information includes matters subject to legal privilege, communications between a Member of the Scottish Parliament (or a Member of Parliament) and another person on constituency matters, confidential personal information, or confidential journalistic material. So, for example, extra care should be taken where, through the use of surveillance, it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter's spiritual welfare, or between a Member of the Scottish Parliament (or a Member of Parliament) and a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality or matters subject to legal privilege may be involved. References to a Member of Parliament include references to Members of both Houses of the UK Parliament and the European Parliament.

4.2. Authorisations under the 1997 Act likely to result in the acquisition of knowledge of matters subject to legal privilege, confidential personal information or confidential journalistic material require (other than in urgent cases) the approval of a Surveillance Commissioner.

4.3. Authorisations for directed surveillance of legal consultations falling within the 2015 Order must comply with the enhanced authorisation regime described below. In cases where it is likely that knowledge of confidential information will be acquired, the use of covert surveillance is subject to a higher level of authorisation.

Material subject to legal privilege: introduction

4.4. Directed surveillance likely or intended to result in the acquisition of knowledge of matters subject to legal privilege may take place in circumstances covered by the 2015 Order, or in other circumstances. Similarly, property interference may be necessary in order to effect surveillance described in the 2015 Order, or in other circumstances where knowledge of matters subject to legal privilege is likely to be obtained. However, where any directed surveillance of a "legal consultation" within the meaning given by the 2015 Order takes place, the provisions of that Order apply as follows.

4.5. The 2015 Order provides that directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in article 3(2) of the Order as is, at any time during the surveillance, used for the purposes of 'legal consultations' is to be treated for the purposes of RIP(S)A as intrusive surveillance.

4.6. The 2015 Order defines 'legal consultation' for these purposes. It means:

- a consultation between a professional legal adviser and that adviser's client or any person representing that client; or
- a consultation between a professional legal adviser or that adviser's client or any person representing that client and a registered medical practitioner, made in connection with, or in contemplation of, legal proceedings and for the purpose of such proceedings.

4.7. The definition of 'legal consultation' in the 2015 Order does not distinguish between legal consultations which are privileged, wholly or in part, and legal consultations which may be in furtherance of a criminal purpose are therefore not protected by any form of privilege. Covert surveillance of all legal consultations covered by the 2015 Order (whether protected by privilege or not) is to be treated as intrusive surveillance.

4.8. Where material is obtained which may contain matters subject to legal privilege legal advice should be taken to determine how that material may be used in evidential terms.

Tests to be applied when authorising or approving covert surveillance or property interference likely or intended to result in the acquisition of knowledge of matters subject to legal privilege

4.9. All applications for covert surveillance or property interference that may result in the acquisition of knowledge of matters subject to legal privilege, within the meaning given by paragraph 1.1 of this code, should state whether the covert surveillance or property interference is intended to obtain knowledge of matters subject to legal privilege.

4.10. If the covert surveillance or property interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it. If the risk cannot be removed entirely, the application should explain what steps will be taken to ensure that any knowledge of matters subject to legal privilege which is obtained is not used in law enforcement investigations or criminal prosecutions.

4.11. Where covert surveillance or property interference is likely or intended to result in the acquisition of knowledge of matters subject to legal privilege, an authorisation shall only be granted or approved if the authorising officer, or approving Surveillance Commissioner, as appropriate, is satisfied that there are exceptional and compelling circumstances that make the authorisation necessary:

- where the surveillance or property interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege, such exceptional and compelling circumstances may arise in the interests of preventing or detecting serious crime;
- where the surveillance or property interference is intended to result in the acquisition of knowledge of matters subject to legal privilege, such

circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb and the surveillance or property interference is reasonably regarded as likely to yield intelligence necessary to counter the threat.

4.12. Further, in considering any authorisation for covert surveillance or property interference likely or intended to result in the acquisition of knowledge of matters subject to legal privilege, the authorising officer and approving Surveillance Commissioner must be satisfied that the proposed covert surveillance or property interference is proportionate to what is sought to be achieved. In relation to intrusive surveillance, including surveillance to be treated as intrusive as a result of the 2015 Order, section 10(2) of RIP(S)A will apply.

4.13. Intrusive surveillance, including surveillance which is treated as intrusive as a result of the 2015 Order, or property interference likely to result in the acquisition of matters subject to legal privilege may only be authorised by authorising officers entitled to grant intrusive surveillance or property interference authorisations.

4.14. Property interference likely to result in the acquisition of such material is subject to prior approval by a Surveillance Commissioner. Intrusive surveillance, including surveillance which is treated as intrusive as a result of the 2015 Order, is subject to prior approval by a Surveillance Commissioner.

Surveillance under the 2015 Order

4.15. As noted above, the 2015 Order provides that directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in article 3(2) of the Order as is, at any time during the surveillance, used for the purposes of 'legal consultations' shall be treated for the purposes of RIP(S)A as intrusive surveillance.

4.16. As a result of the 2015 Order, such surveillance cannot be undertaken without the prior approval of a Surveillance Commissioner.

4.17. The locations specified in the Order are:

(a) any premises in which persons who are serving sentences of imprisonment or detention, remanded in custody or remanded or committed for trial or sentence, may be detained;

(b) legalised police cells within the meaning of section 14(1) of the Prisons (Scotland) Act 1989;

(c) any premises in which persons may be detained under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Borders Act 2007;

(d) any premises in which persons may be detained under Part VI of the Criminal Procedure (Scotland) Act 1995 or the Mental Health (Care and Treatment) (Scotland) Act 2003;

(e) police stations;

(f) the place of business of any professional legal adviser; and.

(g) any premises used for the sittings and business of any court, tribunal or inquiry.

4.18. Authorisations for surveillance which is to be treated as intrusive surveillance as a result of the 2015 Order shall not take effect until such time as:

(a) the authorisation has been approved by a Surveillance Commissioner; and

(b) written notice of the Surveillance Commissioner's decision to approve the authorisation has been given to the authorising officer.

Property interference under the 1997 Act likely to result in the acquisition of knowledge of matters subject to legal privilege

4.19. With the exception of urgent authorisations, where it is believed that the action authorised is likely to result in the acquisition of knowledge of matters subject to legal privilege an authorisation under the 1997 Act shall not take effect until such time as:

a) the authorisation has been approved by a Surveillance Commissioner; and

b) written notice of the Surveillance Commissioner's decision to approve the authorisation has been given to the authorising officer.

The use and handling of matters subject to legal privilege

4.20. Matters subject to legal privilege are particularly sensitive and surveillance which acquires such material may give rise to issues under Article 6 of the ECHR (right to a fair trial) as well as engaging Article 8.

4.21. Where public authorities deliberately acquire knowledge of matters subject to legal privilege, they may use that knowledge to counter the threat which led them to acquire it, but it will not be admissible in court. Public authorities should ensure that knowledge of matters subject to legal privilege, whether or not it is acquired deliberately, is kept separate from law enforcement investigations or criminal prosecutions.

4.22. In cases likely to result in the acquisition of knowledge of matters subject to legal privilege, the authorising officer or Surveillance Commissioner may require regular reporting so as to be able to decide whether the authorisation should continue. In those cases where legally privileged material has been acquired and retained, the matter should be reported to the authorising officer by means of a review and to the Surveillance Commissioner or Inspector during his next inspection (at which the material should be made available if requested).

4.23. A substantial proportion of the communications between a lawyer and his client(s) may be privileged. Therefore, in any case where a lawyer is the subject of an investigation or operation, authorising officers should consider whether the special safeguards outlined in this chapter apply. Any material which has been retained from any such investigation or operation

should be notified to the Surveillance Commissioner or Inspector during his next inspection and made available on request.

4.24. Where there is any doubt as to the handling and dissemination of knowledge of matters which may be subject to legal privilege, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the information takes place. Similar advice should also be sought where there is doubt over whether information is not privileged because it forms part of a communication intended to further a criminal purpose. The retention of privileged material, or its dissemination to an outside body, should be accompanied by a clear warning that it is privileged. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates. Any dissemination of privileged material to an outside body should be notified to the Surveillance Commissioner or Inspector during his next inspection.

Confidential information

4.25. Special consideration must also be given to authorisations that involve confidential personal information, confidential constituent information and confidential journalistic material. Where such material has been acquired and retained, the matter should be reported to the Surveillance Commissioner or Inspector during his next inspection and the material be made available to him if requested.

4.26. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it.[26] Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples include consultations between a health professional and a patient, or information from a patient's medical records.

4.27. Confidential constituent information is information relating to communications between, for example, a Member of the Scottish Parliament (or a Member of Parliament) and a constituent in respect of constituency matters. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.28. Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being

[26] Spiritual counselling means conversations between a person and a religious authority acting in an official capacity, where the individual being counselled is seeking or the religious authority is imparting forgiveness, absolution or the resolution of conscience in accordance with their faith.

acquired for the purposes of journalism and held subject to such an undertaking.

4.29. Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place.

5. Authorisation procedures for directed surveillance

Authorisation criteria

5.1. Under section 6 of RIP(S)A an authorisation for directed surveillance may be granted by an authorising officer where he believes that the authorisation is necessary in the circumstances of the particular case on the grounds that it is:

a) for the purpose of preventing or detecting[27] crime or of preventing disorder;

b) in the interests of public safety;

c) for the purpose of protecting public health[28];

5.2. The authorising officer must also believe that the surveillance is proportionate to what it seeks to achieve (see 3.3-3.12).

Relevant public authorities

5.3. The public authorities entitled to authorise directed surveillance (including to acquire confidential information, with specified higher authorisation), are listed in section 8 of RIP(S)A.

Authorisation procedures

5.4. Responsibility for authorising the carrying out of directed surveillance rests with the authorising officer and requires the personal authority of the authorising officer. The 2010 Order designates the authorising officer for each different public authority and the officers entitled to act in urgent cases.

5.5. An authorising officer must give authorisations in writing, except that in urgent cases they may be given orally by the authorising officer or in writing by the officer entitled to act in urgent cases. In such cases, a record that the authorising officer has expressly authorised the action should be recorded in writing by both the authorising officer and the applicant as soon as is reasonably practicable, together with the information detailed below.

5.6. A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not generally to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's or applicant's own making.

---

[27] Detecting crime is defined in section 31(8) of RIP(S)A and is applied to the 1997 Act by section 134 of that Act (as amended). Preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

[28] This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

5.7. Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an authorising officer authorises such an investigation or operation the centrally retrievable record of authorisations (see Chapter 8) should highlight this and the attention of a Surveillance Commissioner or Inspector should be invited to it during his next inspection.

Information to be provided in applications for authorisation

5.8. A written application for a directed surveillance authorisation should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in Section 6(3) of RIP(S)A;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- a summary of the intelligence case and appropriate unique intelligence references where applicable;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve; and,
- the level of authority required (or recommended where that is different) for the surveillance.

5.9. A subsequent record of whether authorisation was given or refused, by whom, and the time and date this happened should also be recorded.

5.10. In urgent cases, the above information may be supplied orally. In such cases the authorising officer and applicant, where applicable, should record the following information in writing, as soon as is reasonably practicable (it is not necessary to record further detail):

- the identities of those subject to surveillance;
- the nature of the surveillance as defined at 1.9;
- the reasons why the authorising officer considered the case so urgent that an oral instead of a written authorisation was given; and,
- where the officer entitled to act in urgent cases has given written authority, the reasons why it was not reasonably practicable for the application to be considered by the authorising officer should also be recorded.

Duration of authorisations

5.11. A written authorisation granted by an authorising officer will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the day at which it took effect.

5.12. Urgent oral authorisations or written authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after seventy-two hours, beginning with the time when the authorisation was granted.

Renewals

5.13. If, at any time before an authorisation for directed surveillance authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of three months. Renewals may also be granted orally in urgent cases and last for a period of seventy-two hours. The renewal will take effect at the time at which the authorisation would have ceased to have effect but for the renewal.

5.14. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation.

5.15. All applications for the renewal of a directed surveillance authorisation should record (at the time of application, or when reasonably practicable in the case of urgent cases approved orally):

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information in the initial application;
- the reasons why the authorisation for directed surveillance should continue;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

5.16. Authorisations may be renewed more than once, if necessary and provided they continue to meet the criteria for authorisation. The details of any renewal should be centrally recorded (see Chapter 8).

Cancellations

5.17. During a review, the authorising officer who granted or last renewed the authorisation may amend specific aspects of the authorisation, for example, to cease surveillance against one of a number of named subjects or to discontinue the use of a particular tactic. They must cancel the authorisation if satisfied that the directed surveillance as a whole no longer meets the criteria upon which it was authorised. Where the original authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer (see 2010 Order).

5.18. As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained (see Chapter 8). There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation. However effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

Foreign surveillance teams operating in UK

5.19. The provisions of section 76A of RIPA as inserted by the Crime (International Co-Operation) Act 2003 provide for foreign surveillance teams to operate in the UK, subject to the following procedures and conditions.

5.20. Where a foreign police or customs officer[29], who is conducting directed or intrusive surveillance activity outside the UK[30], needs to enter the UK for the purposes of continuing that surveillance, and where it is not reasonably practicable for a UK officer[31] to carry out the surveillance under the authorisation of Part II of RIPA (or of RIP(S)A), the foreign officer must notify a person designated by the Director General of the National Crime Agency immediately after entry to the UK and shall request (if this has not been done already) that an application for a directed or intrusive surveillance authorisation be made under RIPA (or RIP(S)A).

5.21. The foreign officer may then continue to conduct directed or intrusive surveillance for a period of five hours beginning with the time when the officer enters the UK. The foreign officer may only carry out the surveillance, however, in places to which members of the public have or are permitted to have access, whether on payment or otherwise. The directed or intrusive surveillance authorisation, if obtained, will then authorise the foreign officers to conduct such surveillance beyond the five hour period in accordance with the general provisions of RIPA (or RIP(S)A).

[29] as defined in section 76A(10) of RIPA.
[30] With the lawful authority of the country or territory in which it is being carried out and in respect of a suspected crime which falls within Article 40(7) of the Schengen Convention or which is a crime for the purposes of any other international agreement to which the UK is a party and which is specified for the purposes of section 76(A) of the 2000 Act in an order made by the Secretary of State with the consent of Scottish Ministers.
[31] Being a member of a police force, NCA or HMRC.

6. Authorisation procedures for intrusive surveillance

General authorisation criteria

6.1. An authorisation for intrusive surveillance may be granted by the chief constable of the Police Service or the PIRC, as listed in section 10(1A) of RIP(S)A.

6.2. In many cases an operation using covert techniques may involve both directed or intrusive surveillance and property interference. This can be authorised as a combined authorisation, although the criteria for authorisation of each activity must be considered separately (see 3.12-3.14 above on combined authorisations).

6.3. The person mentioned in paragraph 6.1 may only authorise intrusive surveillance if they believe that the authorisation is necessary in the circumstances of the particular case on the grounds that it is for the purpose of preventing or detecting serious crime[32] and that the surveillance is proportionate to what is sought to be achieved by carrying it out. The PIRC may only grant authorisations in relation to an investigation into any circumstances in which there is an indication that a person serving with the police has committed an offence.[33]

6.4. When deciding whether an authorisation is necessary and proportionate, it is important to consider whether the information which it is thought necessary to obtain by means of the intrusive surveillance could reasonably be obtained by other less intrusive means.

Urgent cases

6.5. In relation to the Police Service, the authorising officer should generally give authorisations in writing. However, in urgent cases, oral authorisations may be given by the authorising officer. In an urgent oral case, a statement that the authorising officer has expressly authorised the conduct should be recorded in writing by the applicant as soon as is reasonably practicable, together with the information detailed below.

6.6. In relation to the PIRC, in an urgent case, where it is not reasonably practicable having regard to the urgency of the case for the PIRC to consider the application, an authorisation may be granted in writing by a staff officer of the PIRC designated for that purpose under section 12ZA of RIP(S)A.

6.7. A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the

[32] Serious crime is defined in section 31(6) and (7) as crime that comprises an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

[33] In this context, "person serving with the police" means a constable of the Police Service, a member of the police staff of the Police Service or a member of the staff of the Scottish Police Authority.

authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's or applicant's own making.

Jurisdictional considerations

6.8. The Chief Constable of the Police Service (or a designated senior officer) may only grant an authorisation for intrusive surveillance on an application by a constable of the Police Service. The PIRC may only grant such an authorisation on an application by one of the PIRC's staff officers.

6.9. Where the surveillance is carried out in relation to any residential premises, the authorisation cannot be granted unless the residential premises are in Scotland.

Approval of Surveillance Commissioners

6.10. Except in urgent cases an authorisation granted for intrusive surveillance will not take effect until it has been approved by a Surveillance Commissioner and written notice of the Surveillance Commissioner's decision has been given to the person who granted the authorisation. This means that the approval will not take effect until the notice has been received in the office of the person who granted the authorisation within the relevant public authority.

6.11. When the authorisation is urgent it will take effect from the time it is granted provided notice is given to the Surveillance Commissioner in accordance with section 13(3)(b) (see section 14(2)(b) of RIP(S)A).

6.12. There may be cases that become urgent after approval has been sought but before a response has been received from a Surveillance Commissioner. In such a case, the authorising officer should notify the Surveillance Commissioner in writing that the case is now urgent (pointing out that it has become urgent since the notification). In these cases, the authorisation will take effect immediately.

Notifications to Surveillance Commissioners

6.13. Where a person grants, renews or cancels an authorisation for intrusive surveillance, he must, as soon as is reasonably practicable, give notice in writing to a Surveillance Commissioner, where relevant, in accordance with whatever arrangements have been made by the Chief Surveillance Commissioner.[34]

6.14. In urgent cases, the notification must specify the grounds on which the case is believed to be one of urgency. The urgency provisions should not be used routinely. If the Surveillance Commissioner is satisfied that there

[34] The information to be included in the notification to the Surveillance Commissioner is set out in the Regulation of Investigatory Powers (Notification of Authorisations etc.) (Scotland) Order 2000; SSI No: 340.

were no grounds for believing the case to be one of urgency, he has the power to quash the authorisation.

Information to be provided in all applications for intrusive surveillance

6.15. Applications should be in writing and should describe the conduct to be authorised and the purpose of the investigation or operation. The application should specify:

- the reasons why the authorisation is necessary in the particular case and on the grounds of preventing or detecting serious crime;
- the nature of the surveillance;
- the residential premises or private vehicle in relation to which the surveillance will take place, where known;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any confidential information that is likely to be obtained as a consequence of the surveillance; and
- the reasons why the surveillance is considered proportionate to what it seeks to achieve.

6.16. A subsequent record of whether authorisation was given or refused, by whom, and the time and date this happened should also be recorded.

6.17. In urgent cases, the above information may be supplied orally. In such cases the applicant should record the following information in writing, as soon as is reasonably practicable (it is not necessary to record further detail):

- the identities, where known, of those subject to surveillance;
- the nature and location of the surveillance;
- the reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written authorisation was given; and/or
- the reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

Duration of intrusive surveillance authorisations

6.18. A written authorisation will cease to have effect (unless renewed) at the end of a period of three months, beginning with the day on which it took effect. So an authorisation given at 09.00 on 12 February will expire on 11 May. (Authorisations (except those lasting for 72 hours) will cease at 23.59 on the last day).

6.19. The duration of an authorisation is calculated from the time at which the person who gave the authorisation was notified that the Surveillance Commissioner had approved it. This can be done by presenting the authorising officer with the approval decision page to note in person or if

the authorising officer is unavailable, sending the written notice by auditable electronic means.

6.20. Oral authorisations given in urgent cases and written authorisations given by those only entitled to act in urgent cases, will cease to have effect (unless renewed) at the end of the period of seventy-two hours beginning with the time when they took effect.

Renewals of intrusive surveillance authorisations

6.21. If, at any time before an authorisation expires, the authorising officer considers that the authorisation should continue to have effect for the purpose for which it was issued, he may renew it in writing for a further period of three months.

6.22. As with the initial authorisation, the authorising officer must (unless it is a case to which the urgency procedure applies) seek the approval of a Surveillance Commissioner. The renewal will not take effect until the notice of the Surveillance Commissioner's approval has been received in the office of the person who granted the authorisation within the relevant force or organisation (but not before the day on which the authorisation would have otherwise ceased to have effect).

6.23. In urgent cases, a renewal can take effect immediately (provided this is not before the day on which the authorisation would have otherwise ceased to have effect). See section 13 and 14 of RIP(S)A and the Regulation of Investigatory Powers (Notification of Authorisations etc.) (Scotland) Order 2000; SSI No: 340.

Information to be provided for all renewals of intrusive surveillance authorisations

6.24. All applications for a renewal of an intrusive surveillance authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information listed in paragraph 6.15;
- the reasons why it is necessary to continue with the intrusive surveillance;
- the content and value to the investigation or operation of the product so far obtained by the surveillance;
- the results of any reviews of the investigation or operation (see below).

6.25. Authorisations may be renewed more than once, if necessary, and details of the renewal should be centrally recorded (see Chapter 8).

Cancellations of intrusive surveillance activity

6.26. The senior authorising officer who granted or last renewed the authorisation must cancel it if he is satisfied that the surveillance no longer meets the criteria upon which it was authorised.

6.27. As soon as the decision is taken that intrusive surveillance should be discontinued, the instruction must be given to those involved to stop the intrusive surveillance. The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained (see Chapter 8). There is no requirement to record any further details. However, effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

6.28. Following the cancellation of any intrusive surveillance authorisation the Surveillance Commissioners must be notified of the cancellation.[35]

Authorisations quashed by a Surveillance Commissioner

6.29. In cases where a Police Service or PIRC authorisation is quashed or cancelled by a Surveillance Commissioner, the senior authorising officer must immediately instruct those involved to stop carrying out the intrusive surveillance. Documentation of the date and time when such an instruction was given should be retained for at least three years (see Chapter 8).

[35] This notification shall include the information specified in the Regulation of Investigatory Powers (Notification of Authorisations etc.) (Scotland) Order 2000; SSI No: 340.

7. Authorisation procedures for property interference

General basis for lawful activity

7.1. Authorisations under Part III of the 1997 Act should be sought wherever members of the Police Service or the PIRC conduct entry on, or interference with, property or with wireless telegraphy that would be otherwise unlawful.

7.2. For the purposes of this chapter, "property interference" shall be taken to include entry on, or interference with, property or with wireless telegraphy.

7.3. In many cases an operation using covert techniques may involve both directed or intrusive surveillance and property interference. This can be authorised as a combined authorisation, although the criteria for authorisation of each activity must be considered separately (see 3.12-3.14, on combined authorisations).

Example: The use of a surveillance device for providing information about the location of a vehicle may involve some physical interference with that vehicle as well as subsequent directed surveillance activity. Such an operation could be authorised by a combined authorisation for property interference (under Part III of the 1997 Act) and, where appropriate, directed surveillance (under RIP(S)A). In this case, the necessity and proportionality of the property interference element of the authorisation would need to be considered by the appropriate authorising officer separately to the necessity and proportionality of obtaining private information by means of the directed surveillance.

7.4. A property interference authorisation is not required for entry (whether for the purpose of covert recording or for any other legitimate purpose) into areas open to the public in shops, bars, restaurants, hotel foyers, blocks of flats or any other premises to which, with the implied consent of the occupier, members of the public are afforded unqualified access. Nor is authorisation required for entry on any other land or premises at the invitation of the occupier. This is so whatever the purposes for which the premises are used. If consent for entry has been obtained by deception (e.g. requesting entry for a false purpose), however, an authorisation for property interference should be obtained.

Informed consent

7.5. Authorisations under the 1997 Act are not necessary where the public authority is acting with the informed consent of a person able to give permission in respect of the relevant property and actions. However, consideration should still be given to the need to obtain a directed or intrusive surveillance authorisation under RIP(S)A depending on the operation.

Example: A vehicle is fitted with a security alarm to ensure the safety of an undercover officer. If the consent of the vehicle's owner is obtained to install this alarm, no authorisation under the 1997 Act is required. However, if the owner has not provided consent, an authorisation will be required to render lawful the property interference. The fact that the undercover officer is aware of the alarm installation is not relevant to the lawfulness of the property interference.

Incidental property interference

7.6. RIP(S)A provides that no person shall be subject to any civil liability in respect of any conduct which is incidental to correctly authorised directed or intrusive surveillance activity and for which an authorisation is not capable of being granted or might not reasonably have been expected to have been sought under any existing legislation.[36] Thus a person shall not, for example, be subject to civil liability for trespass where that trespass is incidental to properly authorised directed or intrusive surveillance activity and where an authorisation under the 1997 Act is available but might not reasonably have been expected to be sought (perhaps due to the unforeseeable nature or location of the activity).

7.7. Where an authorisation for the incidental conduct is not available (for example because the 1997 Act does not apply to the public authority in question), the public authority shall not be subject to civil liability in relation to any incidental conduct, by virtue of section 5(2) of RIP(S)A. Where, however, a public authority is capable of obtaining an authorisation for the activity, it should seek one wherever it could be reasonably expected to do so.

Example: Surveillance officers crossing an area of land covered by an authorisation under the 1997 Act are forced to temporarily and momentarily cross into neighbouring land to bypass an unforeseen obstruction, before returning to their authorised route.

Samples

7.8. The acquisition of samples, such as DNA samples, fingerprints and footwear impressions, where there is no consequent loss of or damage to property does not of itself constitute unlawful property interference. However, wherever it is necessary to conduct otherwise unlawful property interference to access and obtain these samples, an authorisation under the 1997 Act would be appropriate. An authorisation for directed or intrusive surveillance would not normally be relevant to any subsequent information, whether private or not, obtained as a result of the covert technique. Once a DNA sample, fingerprint or footwear impression has been obtained, any subsequent analysis of this information will not be surveillance as defined at section 31(2) of RIP(S)A. The appropriate lawful authority in these cases is likely to be the Data Protection Act.

Example 1: Police wish to take fingerprints from a public telephone to identify a suspected criminal who is known recently to have used the telephone. The act of taking the fingerprints would not involve any unlawful property interference so no authorisation under the 1997 Act is required. The subsequent recording and analysis of the information obtained to establish the individual's identity would not amount to surveillance and therefore would not require authorisation under RIP(S)A.

Example 2: Police intend to acquire covertly a mobile telephone used by a suspected criminal, in order to take fingerprints. In this case, the acquisition of the telephone for the purposes of obtaining fingerprints could be authorised under the 1997 Act where it would otherwise be unlawful.

[36] See section 5(2) of RIP(S)A.

Authorisations for property interference by the Police Service and PIRC

7.9. Responsibility for these authorisations rests with the authorising officer as defined in section 93(5) of the 1997 Act[37]. Authorisations require the personal authority of the authorising officer.

7.10. Any person giving an authorisation for entry on or interference with property or with wireless telegraphy under section 93(2) of the 1997 Act must believe that:

- it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime[38]; and
- that the taking of the action is proportionate to what the action seeks to achieve.

7.11. The authorising officer must take into account whether what it is thought necessary to achieve by the authorised conduct could reasonably be achieved by other means.

Collaborative working and regional considerations

7.12. The Chief Constable of the Police Service (or a designated senior officer) may only grant an authorisation for property interference on an application by a constable of the Police Service. The PIRC may only grant such an authorisation on an application by one of the PIRC's staff officers.

7.13. Authorisations for the Police Service and PIRC may only be given for property interference within Scotland (see paragraphs 3.18 and 3.19 above).

7.14. Any person granting or applying for an authorisation to enter on or interfere with property or with wireless telegraphy will also need to be aware of particular sensitivities in the local community where the entry or interference is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment. In this regard, it is recommended that the authorising officers in the Police Service and PIRC should consult a senior officer within the respective organisation in which the investigation or operation takes place where the authorising officer considers that conflicts might arise. The Chief Constable of the Police Service of Northern Ireland should be informed of any surveillance operation undertaken by another law enforcement agency which involves its officers maintaining (including replacing) or retrieving equipment in Northern Ireland.

Authorisation procedures

7.15. Authorisations will generally be given in writing by the authorising officer.

[37] As amended by the Police and Fire Reform (Scotland) Act 2012

[38] An authorising officer in a public authority other than the Security Service shall not issue an authorisation under Part III of the 1997 Act where the investigation or operation falls within the responsibilities of the Security Service. Where any doubt exists a public authority should confirm with the Security Service whether or not the investigation is judged to fall within Security Service responsibilities before seeking an authorisation under Part III of the 1997 Act.

Information to be provided in applications

7.16. Applications to the authorising officer for the granting or renewal of an authorisation must be made in writing (unless urgent) by a police officer or PIRC officer and should specify:

- the identity or identities, where known, of those who possess the property that is to be subject to the interference;
- sufficient information to identify the property subject to entry or interference;
- the nature and extent of the proposed interference;
- the details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why the intrusion is justified;
- details of the offence suspected or committed;
- how the authorisation criteria (as set out above) have been met;
- any action which may be necessary to maintain any equipment, including replacing it;
- any action which may be necessary to retrieve any equipment;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and
- whether an authorisation was given or refused, by whom and the time and date on which this happened.

Notifications to Surveillance Commissioners

7.17. Where a person gives, renews or cancels an authorisation in respect of entry on or interference with property or with wireless telegraphy, he must, as soon as is reasonably practicable, give notice of it in writing to a Surveillance Commissioner, where relevant, in accordance with arrangements made by the Chief Surveillance Commissioner. In urgent cases which would otherwise have required the approval of a Surveillance Commissioner, the notification must specify the grounds on which the case is believed to be one of urgency.

7.18. Notifications to Surveillance Commissioners in relation to the granting, renewal and cancellation of authorisations in respect of entry on or interference with property should be in accordance with the requirements of the Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No. 3241.

Cases requiring prior approval of a Surveillance Commissioner

7.19. In certain cases, an authorisation for entry on or interference with property will not take effect until a Surveillance Commissioner has approved it and the notice of approval has been received in the office of the person who granted the authorisation within the relevant force or organisation. These are cases where the person giving the authorisation believes that:

- any of the property specified in the authorisation:
  - is used wholly or mainly as a dwelling or as a bedroom in a hotel; or
  - constitutes office premises[39]; or
- the action authorised is likely to result in any person acquiring knowledge of:
  - matters subject to legal privilege;
  - confidential personal information; or
  - confidential journalistic material.

Duration of authorisations

7.20. Written authorisations in respect of entry on or interference with property or with wireless telegraphy given by authorising officers will cease to have effect at the end of a period of three months beginning with the day on which they took effect. So an authorisation given at 09.00 on 12 February will expire on 11 May. (Authorisations (except those lasting for 72 hours) will cease at 23.59 on the last day).

7.21. In cases requiring prior approval, the duration of an authorisation is calculated from the time at which the person who gave the authorisation was notified that the Surveillance Commissioner had approved it. This can be done by presenting the authorising officer with the approval decision page to note in person or if the authorising officer is unavailable, sending the written notice by auditable electronic means.

Renewals

7.22. If at any time before the time and day on which an authorisation expires the authorising officer considers the authorisation should continue to have effect for the purpose for which it was issued, he may renew it in writing for a period of three months beginning with the day on which the authorisation would otherwise have ceased to have effect. Authorisations may be renewed more than once, if necessary, and details of the renewal should be centrally recorded (see Chapter 8).

7.23. Where relevant, the Surveillance Commissioners must be notified of renewals of authorisations. The information to be included in the notification is set out in the Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No: 3241.

7.24. If, at the time of renewal, criteria exist which would cause an authorisation to require prior approval by a Surveillance Commissioner, then the approval of a Surveillance Commissioner must be sought before the renewal can take effect. The fact that the initial authorisation required the approval of a Surveillance Commissioner before taking effect does not mean that its renewal will automatically require such approval. It will only do so if, at the time of the renewal, it falls into one of the categories requiring approval (and is not an urgent case).

[39] Office premises are defined as any building or part of a building whose sole or principal use is as an office or for office purposes (which means purposes of administration, clerical work, handling money and telephone or telegraph operation).

Cancellations

7.25. The senior authorising officer who granted or last renewed the authorisation must cancel it if he is satisfied that the authorisation no longer meets the criteria upon which it was authorised. Where the senior authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as the senior authorising officer (see the Regulation of Investigatory Powers (Cancellation of Authorisations) (Scotland) Order 2002; SSI No: 207).

7.26. Following the cancellation of the authorisation, the Surveillance Commissioners must be notified of the cancellation. The information to be included in the notification is set out in the Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No: 3421.

7.27. The Surveillance Commissioners have the power to cancel an authorisation if they are satisfied that, at any time after an authorisation was given or renewed, there were no reasonable grounds for believing that it should subsist. In such circumstances, a Surveillance Commissioner may order the destruction of records, in whole or in part, other than any that are required for pending criminal or civil proceedings.

Retrieval of equipment

7.28. Because of the time it can take to remove equipment from a person's property it may also be necessary for an authorisation to make clear that it also permits the retrieval of anything left on property following completion of the intended action. The notification to Surveillance Commissioners of the authorisation should include reference to the need to remove the equipment and, where possible, a timescale for removal.

7.29. Where a Surveillance Commissioner quashes or cancels an authorisation or renewal, he will, if there are reasonable grounds for doing so, order that the authorisation remain effective for a specified period, to enable officers to retrieve anything left on the property by virtue of the authorisation.

Ceasing of entry on or interference with property or with wireless telegraphy

7.30. Once an authorisation or renewal expires or is cancelled or quashed, the authorising officer must immediately give an instruction to cease all the actions authorised for the entry on or interference with property or with wireless telegraphy. The time and date when such an instruction was given should be centrally retrievable for at least three years (see Chapter 8).

8. Keeping of records

Centrally retrievable records of authorisations

Directed and intrusive surveillance authorisations

8.1. A record of the following information pertaining to all authorisations shall be centrally retrievable within each public authority for a period of at least three years from the ending of each authorisation. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available to the Surveillance Commissioner or an Inspector from the Office of Surveillance Commissioners upon request:

- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice[40];
- whether the authorisation was granted by an individual directly involved in the investigation;[41]
- the date the authorisation was cancelled.

8.2. The following documentation should also be centrally retrievable for at least three years from the ending of each authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction to cease surveillance was given;

[40] See Chapter 4
[41] See paragraph 5.7

- the date and time when any other instruction was given by the authorising officer.

Property interference authorisations

8.3. The following information relating to all authorisations for property interference should be centrally retrievable for at least three years:

- the time and date when an authorisation is given;
- whether an authorisation is in written or oral form;
- the time and date when it was notified to a Surveillance Commissioner, if applicable;
- the time and date when the Surveillance Commissioner notified his approval (where appropriate);
- every occasion when entry on or interference with property or with wireless telegraphy has occurred;
- the result of periodic reviews of the authorisation;
- the date of every renewal; and
- the time and date when any instruction was given by the authorising officer to cease the interference with property or with wireless telegraphy.

8.4. RIP(S)A records must be available for inspection by the Surveillance Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of the Act), particularly where continuing conduct is alleged. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to five years.

9. Handling of material and use of material as evidence

Use of material as evidence

9.1. Subject to the provisions in chapter 4 of this Code, material obtained through directed or intrusive surveillance, or entry on, or interference with, property or wireless telegraphy, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law and is impacted by the Human Rights Act 1998.

9.2. Any decisions by a Surveillance Commissioner in respect of granting prior approval for intrusive surveillance activity or entry on, or interference with, property or with wireless telegraphy, shall not be subject to appeal or be liable to be questioned in any court.[42]

Retention and destruction of material

9.3. Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance or property interference. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

9.4. Where the product of surveillance or interference with property or wireless telegraphy could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

9.5. There is nothing in RIP(S)A or the 1997 Act which prevents material obtained under directed or intrusive surveillance or property interference authorisations from being used to further other investigations.

Law enforcement agencies

9.6. In the cases of the law enforcement agencies, particular attention is drawn to the requirements of Part 6 of the Criminal Justice and Licensing (Scotland) Act 2010. This requires that material which is obtained in the course of a criminal investigation must be provided to the prosecutor.

[42] see section 91(10) of the 1997 Act

10. Oversight by Surveillance Commissioners

10.1. The 1997 Act and RIP(S)A require the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part III of the 1997 Act and RIP(S)A by the Police Service and PIRC, and other public authorities listed in section 8 of RIP(S)A and the 2010 Order.

10.2. This Code does not cover the exercise of any of the Surveillance Commissioners' functions. It is the duty of any person who uses these powers to comply with any request made by a Surveillance Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

10.3. References in this Code to the performance of review functions by the Chief Surveillance Commissioner and other Surveillance Commissioners apply also to Inspectors and other members of staff to whom such functions have been delegated.

11. Complaints

11.1. RIPA establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the Scottish Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction[43]. This Code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

020 7035 3711

[43] See section 23 of RIP(S)A

12. Glossary

Application	A request made to an authorising officer to consider granting (or renewing) an authorisation for directed or intrusive surveillance (under RIP(S)A), or interference with property or wireless telegraphy (under the 1997 Act). An application will be made by a member of a relevant public authority.
Authorisation	An application which has received the approval of an authorising officer. Depending on the circumstances, an authorisation may comprise a written application that has been signed by the authorising officer, or an oral application that has been verbally approved by the authorising officer.
Authorising officer	A person within a public authority who is entitled to grant authorisations under RIP(S)A or 1997 Act Should be taken to include senior authorising officers.
Confidential information	Confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of the Scottish Parliament (and Members of Parliament) and their constituents, or matters subject to legal privilege. See Chapter 4 for a full explanation.
Public authority	Any public organisation, agency or police force.
Private information	Any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. Private information includes information about any person, not just the subject(s) of an investigation.
Member of a public authority	An employee or office holder of a public authority, or a person seconded to that authority.
Senior authorising officer	A person within a public authority who is entitled to grant intrusive surveillance authorisations under RIP(S)A and property interference authorisations under the 1997 Act. See also Authorising officer.

ANNEX A

Authorisation level when knowledge of confidential information is likely to be acquired

Relevant Public Authority	**Authorisation level**
The Police Service of Scotland	The Chief Constable
Police Investigations and Review Commissioner	The Commissioner
The Scottish Government	
Marine Scotland	Chief of Enforcement
Accountant in Bankruptcy	Accountant in Bankruptcy
Scottish Prison Service	Governor in Charge
Contracted out prisons	The controller appointed under section 107(1)(b) of the Criminal Justice and Public Order Act 1994
Transport Scotland	Director
A council constituted under section 2 of the Local Government etc (Scotland) Act 1994	Assistant Head of Service; Investigation manager
The Common Services Agency for the Scottish Health Service Counter	NHSScotland Counter Fraud Services: Director of Practitioner and Fraud Services
The Scottish Environment Protection Agency	Chief Executive Executive Director Chief Officer

ISBN: 978-1-78412-962-0 (web only)

Published by the Scottish Government, Novemeber 2014

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

Produced for the Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
DPPAS40797 (11/14)

w w w . s c o t l a n d . g o v . u k