Covert Surveillance & Property Interference

DRAFT Code of Practice

July 2017

Scottish Government
Riaghaltas na h-Alba
gov.scot

Covert Surveillance and Property Interference
DRAFT Code of Practice

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

Contents

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;
- "IPA" means the Investigatory Powers Act 2016;
- "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;
- "2016 Order" means the Regulation of Investigatory Powers (Prescriptions of Ranks and Positions) (Scotland) Order 2016;
- "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 provides guidance on when an authorisation should be sought, the procedures that must be followed before activity takes place, and on the examination, retention, destruction and disclosure of any information obtained by surveillance activity. The code also provides guidance on entry on, or interference with, property or with wireless telegraphy by public authorities under Part III of the 1997 Act.

1.3. This code is primarily intended for use by the public authorities able to authorise activity under RIP(S)A and Part III of the 1997 Act. It will also allow other interested persons to understand the procedures to be followed by those public authorities. This code is publicly available and should be readily accessible by members of any relevant

DRAFT

public authority[1] seeking to authorise covert surveillance or to authorise entry on, or interference with, property or with wireless telegraphy.

1.4. 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 the 1997 Act relates to the Police Service or the PIRC). This code replaces the previous code of practice issued in 2015. References in this code to provisions in the IPA, including equipment interference, oversight by the Investigatory Powers Commissioner (IPC) and new provisions on combined warrants are applicable with effect from the commencement of those provisions. Until that time, the previous arrangements set out in the code of practice issued in 2015 should be applied.

1.5. RIP(S)A provides that all codes of practice 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, including the Investigatory Powers Tribunal (IPT) established under RIPA, or to the IPC responsible for overseeing the powers conferred by RIP(S)A and the 1997 Act, it may take the provisions of the codes of practice 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.

1.6. Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples 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. The examples should not be taken as confirmation that any particular public authority undertakes the activity described.

1.7. For the avoidance of doubt, the duty to have regard to the code when exercising functions to which the code relates exist regardless of any contrary content of a public authority's internal advice or guidance.

DRAFT

[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).

2. Activity by public authorities to which this code applies

2.1 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.

2.2 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.[2]

2.3 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[3].

2.4 Specifically, covert surveillance may be authorised under RIP(S)A if it is either intrusive or directed[4]:

- 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 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).

2.5 Chapters 5 and 6 of this code provides a fuller description of directed and intrusive surveillance, along with definitions of terms, exceptions and examples. Surveillance carried out solely as part of a targeted equipment interference warrant under the IPA does not require a separate authorisation under RIP(S)A (see paragraphs 2.19 - 2.20 below).

Interference with property and wireless telegraphy

2.6 Part III of the 1997 Act provides for the authorisation of public authorities to enter on or interfere with property or with wireless telegraphy. Chapter 7 of this code provides a fuller description of such authorisations and the interaction with targeted equipment interference warrants provided for in the IPA.

Basis for lawful surveillance activity

2.7 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.

---

[2] See section 31(2) of RIP(S)A.
[3] As defined in section 1(8)(a) of RIP(S)A.
[4] See sections 1(2) and 1 (3) 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.

DRAFT

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.

2.8 RIP(S)A and Part III of the 1997 Act provide a statutory framework under which covert surveillance activity can be authorised and conducted compatibly with Article 8. Where covert surveillance activities are unlikely 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 applicable and this code does not apply. It should be assumed that intrusive surveillance will always result in the obtaining of private information.

2.9 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.

2.10 Chapter 3 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 provided for. Similarly, chapter 7 of this code provides examples of activity for which an authorisation under the 1997 Act is not available.

Relevant public authorities

2.11 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 those listed in section 8 of RIP(S)A;
- intrusive surveillance applications may only be made by those public authorities listed in section 10(1A) of RIP(S)A;
- 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 section 93(5) of the 1997 Act.

Relationship with RIPA

2.12 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.

2.13 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 2007; SI No. 934). RIP(S)A is the appropriate legislation and should be used by Scottish public authorities for all other

DRAFT

surveillance (see paragraphs 3.9 – 3.10 in relation to the recording of telephone or other conversations).

2.14 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.

2.15 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.

2.16 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

2.17 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.

2.18 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.

Activity to which this code does not apply

2.19 This code does not provide for interference with property or wireless telegraphy that is for the purpose of acquiring communications or equipment data within the meaning of section 100 of the IPA, or any other information which would, unless authorised, constitute one or more offences under section 1 to 3A of the Computer Misuse Act. Such conduct should be authorised by a targeted equipment interference warrant under the IPA and covered by the Equipment Interference Code of Practice.

2.20 Applicants for a property interference authorisation will therefore need to consider whether the proposed interference will result in obtaining communications, equipment data or other information, and whether this is the purpose of the authorisation. If the acquisition of communications, equipment data or other information is incidental and not the purpose of the interference, then this activity may be authorised as property interference under the 1997 Act. Alternatively, the Police Service and the PIRC may obtain a targeted equipment interference warrant under the IPA, or use one of their other statutory powers. See also paragraphs 7.1 – 7.3 of this code.

DRAFT

3. Directed and intrusive surveillance overview

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

Directed surveillance[6]

3.2. 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.

3.3. 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. Chapter 5 provides further information about the authorisation of directed surveillance.

Private information

3.4. RIP(S)A states that private information includes any information relating to a person's private or family life[7]. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family[8] and professional or business relationships. Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

3.5. 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[9]. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information

[6] See section 1(2) of RIP(S)A
[7] See section 1(9) of RIP(S)A.
[8] Family should be treated as extending beyond the formal relationships created by marriage or civil partnership.
[9] Note also that a person in police custody will have certain expectations of privacy.

DRAFT

which is on the internet, particularly where accessing information on social media websites. See paragraphs 3.11 to 3.16 for further guidance about the use of the internet as a surveillance tool.

> **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.

3.6. 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.

3.7. 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[10].

> **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.

Specific situations where an intrusive surveillance authorisation is not available

3.8. Section 1(4) of RIP(S)A provide that the use of surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle is not considered to be intrusive surveillance. The use of such devices 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

[10] 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.

DRAFT

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 about the occupants of the vehicle, could interfere with Article 8 rights. A directed surveillance authorisation may therefore be appropriate[11]. A property interference authorisation may also be appropriate for the covert installation of the device.

Recording of telephone conversations

3.9. The interception of communications sent by public post, or by means of public telecommunications systems, or private telecommunications is governed by Part 2 of the IPA. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the IPA.

3.10. 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 2 of the IPA 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.

Online covert activity

3.11. The internet may be used as a surveillance tool, and where online research or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (see Covert Human Intelligence Sources code of practice).

3.12. In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, if reasonable steps have been taken to inform the public or particular individuals that the surveillance

[11] The use of such devices is also likely to require an authorisation for property interference under the 1997 Act. See Chapter 7.

is or may be taking place this can be regarded as overt and a directed surveillance authorisation will not normally be available.

3.13. Public use of the internet has expanded rapidly so that far more activity and interaction now occurs online than ever before. As set out in paragraph 3.5, there may be a reduced expectation of privacy for material accessible on the internet, but privacy considerations may still apply, for example to information posted on social networking sites where the information may include or constitute private information. This is regardless of whether or not the account holder has applied any privacy settings to the account.

3.14. Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information. However, information posted on personal social networking sites which are normally accessed by a smaller circle of personal contacts is likely to include private information to which an expectation of privacy would apply and fall within the scope of a person's private life. Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and storing information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6.

> **Example:** A simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence is unlikely to need an authorisation. If, however, having found an individual's social media profile or identity it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered. Visiting a website would not normally amount to surveillance, but if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.

3.15. In order to determine whether a directed surveillance authorisation is required for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include whether:

- the investigation or research is directed towards an individual or group of people;

- it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.14);
- it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- the information obtained will be recorded and stored;
- the information is likely to provide an observer with a pattern of lifestyle;
- the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- it is likely to involve identifying and recording information about third parties such as friends and family members of the subject of interest, or information posted by third parties such as friends or family members, which may include private information and therefore constitute collateral intrusion.

3.16. Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.31).

> **Example:** Police researchers using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. If, however, specific names or other identifiers of an individual or group are applied to the search, an authorisation should be considered.

Aerial surveillance

3.17. Where surveillance using airborne crafts or devices, for example helicopters or drones, is planned, the same considerations outlined in chapters 3 and 5 of this code should be made to determine whether a directed surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude.

> **Example**: A drone deployed by a police force to monitor a known group of individuals at a public demonstration is likely to require an authorisation for directed surveillance, as it is likely that private information will be obtained and the observees are unaware it is taking place, regardless of whether the drone is marked as belonging to the police force, unless sufficient steps have been taken to ensure that participants in the demonstration are aware that aerial surveillance will be taking place, such activity should be regarded as covert.

Intrusive surveillance

3.18. 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[12]. If surveillance activity falls within the definition of intrusive surveillance, this has the effect of reducing the number of public authorities able to authorise such surveillance, principally to the Police Service and the PIRC. It will also make authorisations in respect of such surveillance subject to prior approval by a Judicial Commissioner.

3.19. 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 as it is assumed that intrusive surveillance will always be likely to result in the obtaining of private information. Accordingly, it is not necessary to consider whether or not intrusive surveillance is likely to result in the obtaining of private information.

3.20. In addition, directed surveillance under the ambit of the 2015 Order is to be treated as intrusive surveillance[13].

Residential premises

3.21. 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.[14] 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.[15]

3.22. 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[16].

3.23. 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.

3.24. 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;

[12] See section 1(3) of RIP(S)A
[13] The 2015 Order makes provision for surveillance carried out on premises when those premises are used for a legal consultation
[14] See section 31(1) of RIP(S)A
[15] See section 31(9) of RIP(S)A
[16] See section 31(10) of RIP(S)A

DRAFT

- residential premises occupied by a public authority for non-residential purposes.

Private vehicles

3.25. 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[17].

Places for Legal Consultation

3.26. 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;
>
> (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

3.27. 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.[18]

> **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.

[17] See section 31(1) and 31(9) of RIP(S)A.
[18] See section 1(5) of RIP(S)A.

DRAFT

Circumstances where a covert surveillance authorisation is not available

3.28. 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 obtained 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;
- covert surveillance authorised as part of a targeted equipment interference warrant under the IPA;
- certain other specific situations (see paragraphs 2.19 - 2.20).

3.29. Each situation is detailed and illustrated below.

Immediate response

3.30. 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 or monitor social media accounts during a public order incident.

General observation activities

3.31. 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. General observation duties may include monitoring of publicly accessible areas of the internet which is not part of a specific investigation or operation.

> **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:** Police officers monitoring publicly accessible information on social media websites for information using the search term “theft” would not normally

DRAFT

require a directed surveillance authorisation. If, however, they were seeking information relating to a particular individual or group of individuals, for example by using the search term "group x", even where the true identity of those individuals is not known, this may require authorisation. This is because use of a specific search term such as this indicates that the information is being gathered as part of a specific investigation or operation particularly where information is recorded and stored for future use.

Example 3: 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 4: 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

3.32. 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.

3.33. A public authority may only engage in the 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 1: 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[19].

[19] For further information see www.ico.org.uk

DRAFT

Example 2: It is alleged that a public official has brought their department into disrepute by making defamatory remarks online, and identifying themselves as a public official. The department wishes to substantiate the allegations separately from any criminal action. 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 department's core functions.

CCTV and ANPR (Automatic Number Plate Recognition) cameras

3.34. 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[20], 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.

3.35. The Protection of Freedoms Act 2012 requires that a Surveillance Camera Code[21] 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 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.

3.36. Where, however, 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.

DRAFT

[20] For example, by virtue of cameras or signage being clearly visible.

[21] http://ico.org.uk/for_the_public/topic_specific_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/cctv-code-of-practice.pdf

Specific situations where authorisation is not available

3.37. 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[22];
- 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[23];
- 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 available;
- 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)[24].

Covert surveillance authorised by an equipment interference warrant

3.38. The obtaining of communications or information authorised by a targeted equipment interference warrant issued under Part 5 of the IPA includes obtaining those communications or information by surveillance. This could include intrusive surveillance or directed surveillance.

3.39. A separate authorisation for surveillance under RIP(S)A will not therefore be required providing the conduct comprising the surveillance is properly authorised by a targeted equipment interference warrant. The interference with privacy and property resulting from the surveillance will be considered as part of the equipment interference authorisation.

3.40. By contrast, where the surveillance is not linked to the communications, equipment data or other information obtained from the equipment interference, this will not be capable of authorisation under a targeted equipment interference warrant.

3.41. For example, if an agency capable of authorising equipment interference wishes to conduct separate surveillance by directing an officer to observe the user of a device at the same time as the device itself is being subject to equipment interference, then this will not be considered as part of the equipment interference authorisation and an appropriate surveillance authorisation must be obtained. In this situation a combined warrant may be appropriate (for information on combined warrants, see paragraphs 4.19 – 4.27).

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

Foreign surveillance teams operating in UK

3.42. 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.

3.43. Where a foreign police or customs officer[25], who is conducting directed or intrusive surveillance activity outside the UK[26], needs to enter the UK for the purposes of continuing that surveillance, and where it is not reasonably practicable for a UK officer[27] 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).

3.44. 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).

DRAFT

[25] As defined in section 76A(10) of RIPA

[26] 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 RIPA in an Order made by the Secretary of State with the consent of the Scottish Ministers.

[27] Being a member of a police force, NCA or HMRC.

4. General rules on authorisations

Overview

4.1. 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.

4.2. Responsibility for granting authorisations under RIP(S)A 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 and the 2016 Order.

4.3. The statutory purposes for which covert surveillance or property interference authorisations may be issued reflect the functions of the agency carrying out the surveillance or property interference. Operations must be conducted in accordance with the statutory or other functions of the relevant public authority.

Necessity and proportionality

4.4. RIP(S)A and the 1997 Act stipulates 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.[28]

4.5. 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.

4.6. 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.

4.7. 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;

[28] 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.

DRAFT

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

4.8. 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.

DRAFT

Collateral intrusion

4.9. Before authorising applications for directed or intrusive surveillance or property interference, 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).

4.10. 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 or property interference 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 or property interference.

4.11. 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.

4.12. In order to give proper consideration to collateral intrusion, an authorising officer should be given full information regarding the potential scope of the anticipated surveillance or property interference, including the likelihood that any equipment or software deployed may cause intrusion on persons other than the subject(s) of the surveillance or property interference. If an automated system such as an online search engine is used to obtain the information, the authorising officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims for the operation should be discarded or securely retained separately where it may be required for future evidential purposes. The authorising officer should ensure appropriate safeguards for the handling, retention or destruction of such material in accordance with chapter 8 of this code.

4.13. Where a public authority intends to use surveillance tools for testing or training purposes, and to the extent that deployment of those tools in an operational setting is unavoidable, this should be treated as a specific operation for the purposes of the 1997 Act or RIP(S)A including full consideration of the proportionality of any collateral intrusion.

4.14. 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 3.4 - 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.

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

Example: If an individual provides the Police Service with passwords and log-in details for their personal social networking accounts in order to provide evidence of threats made against them, this would not normally require a directed surveillance authorisation. If the Police Service then decided to monitor the accounts for the purposes of obtaining further evidence of criminal activity by the author of the threats, they should consider applying for a directed surveillance authorisation. This is because the Police Service would be acting with the intention to monitor an individual who has not consented to and may not be aware of the surveillance, in circumstances where private information is likely to be obtained. The Police Service will also need to consider the extent of the collateral intrusion into the privacy of others who may comment on or post information onto the accounts under surveillance.

Combined authorisations[29]

4.16. A single authorisation may combine:

- any number of authorisations under RIP(S)A[30];
- an authorisation under RIP(S)A and an authorisation under Part III of the 1997 Act.

4.17. 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 Judicial Commissioner, unless the case is urgent.

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

Combinations involving warrants under the Investigatory Powers Act 2016

4.19. Where an authorisation under RIP(S)A or the 1997 Act is combined with a warrant under the IPA, the authorisation processes in the IPA will apply. In some cases this will necessitate a higher authorisation process than would otherwise be required for individual applications. Where two warrants or authorisations are combined that would

[29] Schedule 8 of the IPA also makes separate provision for combination of warrants and authorisations. This could result in authorisation being given for conduct under the IPA, combined with RIP(S)A.
[30] See section 19(2) of RIP(S)A.

otherwise be issued by different authorities (for example, a property interference authorisation issued by the Police Service and an interception warrant issued by the Scottish Ministers), the warrant will always be issued by the higher authority level. Where one of the warrants or authorisations within a combined warrant is cancelled, the whole warrant ceases to have effect. For example, if conduct required for an operation was authorised by a combined property interference and interception warrant and interception was no longer necessary and proportionate, the whole warrant must be cancelled and a new property interference authorisation sought to cover the property interference that remains necessary and proportionate. Such combined warrants may also be applied for on an urgent basis.

4.20. Where warrants of different durations are combined, the shortest duration applies.

4.21. The requirements that must be met before a warrant can be issued apply to each part of a combined warrant. So, for example, where a combined warrant includes a property interference warrant, all the requirements that would have to be met for a property interference warrant to be issued should be met by the combined warrant.

4.22. The duties imposed by section 2 of the IPA (having regard to privacy) apply to combined warrants as appropriate. The considerations that apply when deciding whether to issue, renew, cancel or modify a warrant under the IPA will apply when such a warrant forms part of a combined warrant. So the property interference or surveillance element of a combined warrant cannot be issued without having regard to privacy in accordance with section 2 of the IPA.

4.23. In seeking the assistance of a third party to give effect to a warrant it is possible to serve only the relevant part of a combined warrant. For example, if a combined warrant included a targeted equipment interference warrant and an authorisation for directed surveillance, and the target equipment interference required the assistance of a third party, it is possible to serve just the part of the warrant that relates to the targeted equipment interference warrant on that third party.

4.24. Paragraph 20 of Schedule 8 to the IPA provides that various rules regarding warrants apply separately to the relevant part of a combined warrant. The duty of operators to give effect to a warrant applies separately in relation to each part of a combined warrant. So, for example, section 128 of the IPA (duty of operators to assist with implementation) would apply to the targeted equipment interference part of a combined warrant but only to that part.

4.25. Similarly, safeguards also apply to individual parts of a combined warrant. For instance, where a combined targeted equipment interference and intrusive surveillance authorisation has been issued, the safeguards that apply to a targeted equipment interference warrant apply to the part of the combined warrant that is a targeted equipment interference warrant. Section 132 (duty not to make unauthorised disclosures) and 134 (the offence of making unauthorised disclosures) of the IPA apply to the targeted equipment interference part of a combined warrant.

4.26. The exclusion of matters from legal proceedings (section 56 of the IPA) continues to apply to an interception warrant that is part of a combined warrant. However, when a property interference or surveillance warrant is combined with an interception warrant the material derived from property interference or surveillance may still in principle be used in legal proceedings if required. However, if material derived from property

interference or surveillance authorised by a combined warrant reveals the existence of an interception warrant the material is excluded from use in legal proceedings according to section 56 of the IPA.

4.27. Should the exclusion from legal proceedings mean that there may be difficulties in disclosing any material obtained under a combined warrant that included an interception warrant, public authorities may wish to consider the possibility of seeking individual warrants instead.

Collaborative working

4.28. 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.

4.29. 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.

4.30. 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.

4.31. In some circumstances it may be appropriate or necessary for a public authority to work with third parties who are not themselves a public authority (such as an individual company or non-governmental organisation) to assist with an investigation or piece of research. Where that third party is acting in partnership with or under the direction of a public authority, then they are acting as an agent of that authority and any activities that third party conducts 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 by the public authority on whose behalf the activity is being undertaken. Similarly, a surveillance authorisation should also be considered where the public authority is aware that a third party is independently conducting surveillance and the public authority intends to make use of any suitable material obtained by the third party for the public authority's own investigative purposes.

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

DRAFT

4.33. 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.

DRAFT

Reviewing authorisations

4.34. 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. 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.

4.35. 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.

4.36. The authorising officer is usually best placed to assess whether the authorisation should continue or whether the criteria on which he or she 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.

4.37. Any proposed or unforeseen changes to the nature or extent of the activity 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.

4.38. 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”.

4.39. During a review, the authorising officer who granted or last renewed the authorisation may amend specific aspects of the authorisation, for example, to cease directed surveillance against one of a number of named subjects or to discontinue the use of a particular tactic.

DRAFT

General best practices

4.40. 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[31];
- the case for the authorisation should be presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;
- 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.

4.41. Furthermore, it is considered good practice that within every relevant public authority, a senior responsible officer[32] 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 IPC and Inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Judicial Commissioner.

Local authorities

4.42. 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 IPC. Where an inspection report highlights concerns about the

[31] As laid out in Chapters 5, 6 and 7 of this code.
[32] The senior responsible officer should be a person holding the office, rank or position of an authorising officer within the relevant public authority.

DRAFT

standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed.

4.43. 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.

DRAFT

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[33] crime or of preventing disorder;

b) in the interests of public safety;

c) for the purpose of protecting public health[34];

5.2. The authorising officer must also believe that the surveillance is proportionate to what it seeks to achieve (see paragraphs 4.4 - 4.8).

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.

Information to be provided in applications for authorisation

5.4. 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;
- where the purpose, or one of the purposes, of the authorisation is to obtain information subject to legal privilege, an assessment of why there are exceptional and compelling circumstances that make this necessary;

[33] 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.

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

DRAFT

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

Authorisation procedures

5.5. Responsibility for authorising the carrying out of directed surveillance rests with the authorising officer and requires the personal authority of the authorising officer. An authorising officer must give authorisations in writing, except in urgent cases when they may be given orally by the authorising officer or in writing by the officer able to act in urgent cases.

5.6. The 2010 Order and the 2016 Order, designate the authorising officer for each different public authority and the officers able to authorise in urgent cases.

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 7) should highlight this and the attention of a Judicial Commissioner or Inspector should be invited to it during his next inspection.

Urgent cases

5.8. The authorising officer should generally give authorisations in writing. However, in urgent cases, oral authorisations may be given by the authorising officer (a person designated only for the purposes of urgent situations must give their authorisation in writing). In an urgent oral case, a statement that the senior authorising officer or designated deputy has expressly authorised the conduct should be recorded in writing by the applicant as soon as is reasonably practicable, together with the information detailed at paragraph 5.10.

5.9. 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.

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 paragraph 2.4 of this code;
- the reasons why the authorising officer considered the case so urgent that an oral instead of a written authorisation was given; and,

DRAFT

- 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 when the authorisation granted has taken 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 72 hours, beginning with the time when the authorisation granted had taken effect.

Renewals

5.13. Section 19 of RIP(S)A provides that authorisations for directed surveillance may be renewed where the authorising officer considers that the authorisation continues to be necessary and proportionate. This may include where an investigation continues after the initial period of authorisation.

5.14. 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 72 hours. The renewal will take effect at the time at which the authorisation would have ceased to have effect but for the renewal.

5.15. 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.

5.16. 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.

5.17. Authorisations may be renewed more than once, if necessary and proportionate, and provided they continue to meet the criteria for authorisation. The details of any renewal should be centrally recorded.

5.18. Where there is a renewal application in respect of an authorisation which has resulted in the obtaining of legally privileged items, that fact should be highlighted in the renewal application. If it is likely that legally privileged items will continue to be

DRAFT

obtained, the renewal should be authorised at the higher level as required by Annex A to this code, and, potentially, by the 2015 Order.

Cancellations

5.19. The authorising officer must cancel the authorisation at any time if they consider that the directed surveillance 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.

5.20. Those acting under an authorisation must keep their authorisations under review and notify the authorising officer if they consider that the authorisation is no longer necessary or proportionate, and so should therefore be cancelled.

5.21. 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) as soon as reasonably practicable. The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained. 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.

DRAFT

6. Authorisation procedures for intrusive surveillance

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 paragraphs 4.16 – 4.18 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[35] 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[36].

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.

Information to be provided in applications

6.5. 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;

DRAFT

[35] Serious crime is defined in section 31(6) and (7) of RIP(S)A 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.

[36] 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.

- where the purpose, or one of the purposes, of the authorisation is to obtain information subject to legal privilege, an assessment of why there are exceptional and compelling circumstances that make this necessary;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve; and
- a subsequent record of whether authorisation was given or refused, by whom, and the time and date this happened should also be recorded.

Urgent cases

6.6. 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.

6.7. 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.

6.8. 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 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.

6.9. 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, including a clear indication of the criminality under investigation;
- 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.

Notifications to a Judicial Commissioner

6.10. 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 Judicial Commissioner, where relevant, in accordance with whatever arrangements have been made by the IPC.

6.11. 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

DRAFT

the Judicial Commissioner is satisfied that there were no grounds for believing the case to be one of urgency, he has the power to quash the authorisation.

Judicial Commissioner approval

6.12. Except in urgent cases an authorisation granted for intrusive surveillance will not take effect until it has been approved by a Judicial Commissioner and written notice of the Judicial 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.

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

6.14. There may be cases that become urgent after approval has been sought but before a response has been received from a Judicial Commissioner. In such a case, the authorising officer should notify the Judicial 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.

Duration of intrusive surveillance authorisations

6.15. 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.

6.16. The duration of an authorisation is calculated from the time at which the person who gave the authorisation was notified that a Judicial 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.

6.17. 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 72 hours beginning with the time when they took effect.

Renewals of intrusive surveillance authorisations

6.18. 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.

6.19. 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 Judicial Commissioner. The renewal will not take effect until the notice of the Judicial 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).

DRAFT

6.20. 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 sections 13 and 14 of RIP(S)A and the Regulation of Investigatory Powers (Notification of Authorisations etc.) (Scotland) Order 2000; SSI No: 340.

6.21. Where there is a renewal application in respect of an authorisation which has resulted in the obtaining of legally privileged items, that fact should be highlighted in the renewal application.

Information to be provided for all renewals of intrusive surveillance authorisations

6.22. 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;
- where the purpose, or one of the purposes, of the authorisation is to obtain information subject to legal privilege, an assessment of why there continue to be exceptional and compelling circumstances that make this necessary;
- 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).

6.23. Authorisations may be renewed more than once, if necessary, and details of the renewal should be centrally recorded.

Cancellations of intrusive surveillance activity

6.24. 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.

6.25. 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. 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.

6.26. Following the cancellation of any intrusive surveillance authorisation the Judicial Commissioners must be notified of the cancellation.[37]

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

DRAFT

Authorisations quashed by a Judicial Commissioner

6.27. In cases where a Police Service or PIRC authorisation is quashed or cancelled by a Judicial 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).

Jurisdictional considerations

6.28. 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.

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

DRAFT

7. Authorisation procedures for property interference

Authorisation criteria

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[38].

7.2. For the purposes of this chapter, "property interference" shall be taken to include entry on, or interference with, property. As noted at paragraphs 2.19 – 2.20, however, these property interference powers cannot be used where the proposed interference is for the purpose of acquiring communications, equipment data or other information. In those circumstances the Police Service and the PIRC are required to apply for an equipment interference warrant under Part 5 of the IPA where the conduct would otherwise constitute an offence under the Computer Misuse Act 1990 (see section 14 of the IPA).

7.3. For example, one of the law enforcement agencies recognises that the process by which it disables a particular CCTV camera results in it obtaining a stored copy of footage from the CCTV system. In such circumstances, although the agency is interfering with equipment (the CCTV system) and acquiring communications and/or private information, the purpose of the interference is to disable the CCTV camera. The acquisition of the CCTV footage is intended, in so far as it is a constituent part of the interference required to disable the CCTV camera, but is entirely incidental. Accordingly, this activity can continue to be authorised as property interference under the 1997 Act (as applicable).

7.4. This can be contrasted with where an agency is seeking to monitor the movements of a target who has been captured on CCTV footage. In such circumstances, the agency interferes with the CCTV system for the purpose of acquiring a copy of the footage; the purpose of the interference with the equipment is to acquire communications and/or private information and a targeted equipment interference warrant would be required.

7.5. Further details on equipment interference warrants are provided in the Equipment Interference Code of Practice.

7.6. 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 paragraphs 4.16 – 4.18 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).

[38] The IPA provides that a person may not, for the purpose of obtaining communications, private information or equipment data, make an application under section 93 of the Police Act 1997 for authorisation to engage in conduct which could be authorised by a targeted equipment interference warrant under part 5 of the IPA if the applicant considers that the conduct would (unless done with lawful authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990

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.

7.7. 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.

7.8. There may be circumstances where both a property interference and equipment interference warrant or authorisation may be required (see paragraphs 4.19 to 4.27 on combined warrants).

Information to be provided in applications

7.9. Applications to the authorising officer for the granting or renewal of an authorisation must be made in writing 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;
- where the purpose, or one of the purposes, of the authorisation or warrant is to obtain information subject to legal privilege, an assessment of why there are exceptional and compelling circumstances that make this necessary;
- 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.

DRAFT

Authorisations for property interference by the Police Service and PIRC

7.10. Authorisations will be given in writing, and responsibility for these authorisations rests with the authorising officer as defined in section 93(5) of the 1997 Act[39]. Authorisations require the personal authority of the authorising officer.

7.11. 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[40]; and
- that the taking of the action is proportionate to what the action seeks to achieve.

7.12. 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 less intrusive means.

Notifications to a Judicial Commissioner

7.13. 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 Judicial Commissioner, where relevant (see paragraph 7.15), in accordance with arrangements made by the IPC. In urgent cases which would otherwise have required the approval of a Judicial Commissioner, the notification must specify the grounds on which the case is believed to be one of urgency.

7.14. Notifications to a Judicial Commissioner 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[41].

Judicial Commissioner approval

7.15. In certain cases, an authorisation for entry on or interference with property will not take effect until a Judicial 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

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

[40]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.

[41] SI 1998/3241

DRAFT

- constitutes office premises[42]; 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

7.16. 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.

7.17. 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 a Judicial Commissioner has 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

7.18. 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. When considering whether to renew an authorisation, the authorising officer must consider whether authorisation remains both necessary and proportionate, with particular regard to whether the length of the operation means continued interference remains proportionate. Authorisations may be renewed more than once, if necessary, and details of the renewal should be centrally recorded. An application for renewal should not be made until shortly before the authorisation period is drawing to an end while allowing an appropriate period of time for any Judicial Commissioner approval that may be required.

7.19. Where relevant, a Judicial Commissioner 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.

7.20. If, at the time of renewal, criteria exist which would cause an authorisation to require prior approval by a Judicial Commissioner, then the approval of a Judicial Commissioner must be sought before the renewal can take effect.

7.21. Where there is a renewal application in respect of an authorisation which has resulted in the obtaining of legally privileged items, that fact should be highlighted in the renewal application.

[42] 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).

DRAFT

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

7.22. Interference should cease as soon as it is determined that a cancellation may be required. 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.

Cancellations

7.23. The senior authorising officer who granted or last renewed the authorisation may cancel an authorisation at any time, but must cancel it if they consider that it is 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.

7.24. As soon as the decision is taken that the interference should be discontinued, the instruction must be given to those involved to stop all such activity as soon as is reasonably practicable.

7.25. Following the cancellation of the authorisation, the Judicial 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:3241.

7.26. The Judicial Commissioners have the power to quash 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 Judicial 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

7.27. 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 Judicial Commissioners of the authorisation should include reference to the need to remove the equipment and, where possible, a timescale for removal.

7.28. Where a Judicial 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.

Informed consent

7.29. 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.

DRAFT

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

7.30. 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.[43] 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).

7.31. 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

7.32. 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 1998.

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

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

DRAFT

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.

Collaborative working and regional considerations

7.33. 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.

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

7.35. Any person granting or applying for an authorisation to enter on or interfere with property 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.

DRAFT

8. Safeguards (including privileged or confidential information)

Introduction

8.1. This chapter provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through directed or intrusive surveillance under RIP(S)A, or property interference under the 1997 Act. This material may include private information as defined in section 1(9) of RIP(S)A. It also details the procedures and safeguards to be applied where authorisations may result in the acquisition of material subject to legal privilege, or other confidential material including journalistic material and the constituency business of a member of a relevant legislature[44].

8.2. Where this chapter refers to material obtained through property interference it should be noted that the activity authorised by a property interference authorisation would not normally consist in the acquisition of information. Where the purpose of any interference with property or wireless telegraphy is to obtain communications, private information or equipment data this would normally fall to be authorised as equipment interference under the IPA. Material obtained through such interference is subject to equivalent safeguards set out in the equipment interference code of practice, and the provisions of this chapter do not apply.

8.3. Public authorities should ensure that their actions when handling information obtained by means of covert surveillance or property interference comply with relevant legal frameworks and this code so that any interference with privacy is justified in accordance with Article 8(2) of the ECHR. Compliance with these legal frameworks will ensure that the handling of private information so obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards.

8.4. All material obtained under the authority of a covert surveillance or property interference authorisation must be handled in accordance with safeguards which the public authority has implemented in line with the requirements of this code. These safeguards should be made available to the IPC. Breaches of these safeguards must be reported to the IPC in a fashion agreed with the IPC. Public authorities must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, public authorities must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

8.5. Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of this code, something is necessary for the authorised purposes if the material:

- is, or is likely to become, necessary for any of the statutory purposes set out in RIP(S)A or the 1997 Act in relation to covert surveillance or property interference;
- is necessary for facilitating the carrying out of the functions of public authorities under those Acts;
- is necessary for facilitating the carrying out of any functions of the IPC or the IPT;

[44] 'A members of a relevant legislature' means a member of the Scottish Parliament, a member of either House of Parliament, a member of the National Assembly for Wales, a member of the Northern Ireland Assembly, or a member of the European Parliament elected for the UK.

- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

8.6. There is nothing in RIP(S)A or the 1997 Act which prevents material obtained under covert surveillance or property interference authorisations from being used to further other investigations where it becomes relevant and in accordance with the safeguards in this Chapter.

Use of material as evidence

8.7. Subject to the provisions in this chapter, material obtained through covert surveillance or property interference 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.

8.8. Any decisions by a Judicial Commissioner in respect of granting prior approval for intrusive surveillance activity or property interference as required under RIP(S)A or the 1997 Act, shall not be subject to appeal or be liable to be questioned in any court[45].

8.9. Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are important and will apply to any material acquired through covert surveillance or property interference that is intended or likely for use in evidence. When information obtained under a covert surveillance or property interference authorisation is used evidentially, the public authority should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

8.10. Where the product of surveillance or property interference could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements.

Reviewing warrants and authorisations

8.11. Regular reviews of all authorisations should be undertaken during their lifetime to assess the necessity and proportionality of the conduct. Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or particularly sensitive information is likely to be obtained. At the point the public authority is considering applying for an authorisation, they must have regard to whether the level of protection to be applied in relation to information obtained under the warrant or authorisation is higher because of the particular sensitivity of that information.

8.12. In each case, unless specified by a Judicial Commissioner, the frequency of reviews should be determined by the public authority that made the application. This should be as frequently as is considered necessary and proportionate.

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

[45] See section 91(10) of the 1997 Act and section 2(10) of RIP(S)A

Handling material

8.14. Paragraphs 8.15 to 8.21 provide guidance as to the safeguards which govern the dissemination, copying, storage and destruction of private information obtained through covert surveillance or property interference. Each public authority must ensure that there are internal arrangements in force for securing that the requirements of these safeguards are satisfied in relation to private information obtained by these means. 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 internal arrangements produced by individual authorities relating to the handling and storage of material.

Dissemination of information

8.15. Material acquired through covert surveillance or property interference may need to be disseminated both within and between public authorities, as well as to consumers of intelligence (which includes the IPC, for example), where necessary in order for action to be taken on it. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary for the authorised purpose set out in paragraph 8.5 above. This obligation applies equally to disclosure to additional persons within a public authority and to disclosure outside the authority. In the same way, only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

8.16. The obligations apply not just to the original public authority acquiring the information under a warrant or authorisation, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the original authority's permission before disclosing the material further. In others, explicit safeguards should be applied to secondary recipients.

8.17. Where material obtained under an authorisation is disclosed to the authorities of a country or territory outside the UK, the public authority must ensure that the material is only handed over to the authorities if it appears to them that any requirements relating to minimising the extent to which material is disclosed, copied, distributed and retained will be observed to the extent that the authorising officer or Judicial Commissioner considers appropriate.

Copying

8.18. Material obtained through covert surveillance or property interference may only be copied to the extent necessary for the authorised purpose. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance or property interference, and any record which refers to the covert surveillance or property interference and the identities of the persons to whom the material relates.

Storage

8.19. Material obtained through covert surveillance or property interference and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material.

8.20. In particular, each public authority must apply the following protective security measures:

- physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems; and
- an appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

8.21. Information obtained through covert surveillance or property interference, and all copies, extracts and summaries thereof, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose set out in paragraph 8.5. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible[46].

Confidential or privileged material

8.22. RIP(S)A does not provide any special protection for 'confidential information'. The 1997 Act makes special provision for certain categories of confidential information. Nevertheless, in all circumstances particular consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality.

8.23. 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 Judicial Commissioner.

Directed surveillance of legal consultations

8.24. Authorisations for directed surveillance of legal consultations falling within the 2015 Order must comply with the enhanced authorisation regime described in paragraphs 8.43 - 8.51. 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[47].

Confidential personal information and confidential constituent information

8.25. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above 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. For example, confidential

[46] For example, by taking reasonable steps to make the data unavailable or inaccessible to authorised persons. No further steps are required, such as physical destruction of hardware.
[47] See Annex A of this code

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

8.26. Spiritual counselling means conversations between an individual and a Minister of Religion acting in his or her official capacity, and where the individual being counselled is seeking, or the Minister is imparting, forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

8.27. Confidential constituent information is information relating to communications between a member of a relevant legislature (see paragraph 8.1) and a constituent member in respect of constituency business. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. If the information is exchanged with the intention of furthering a criminal purpose, for example, then the information will not be considered confidential for the purposes of this code.

8.28. Where the intention is to acquire confidential personal information, or confidential constituent information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered by the authorising officer in accordance with the safeguards in this chapter. If the acquisition of confidential personal or constituent information is likely, but not intended, any possible mitigating steps should be considered by the authorising officer and, if none are available, consideration should be given to whether special handling arrangements are required within the relevant public authority.

8.29. Material which has been identified as confidential personal or constituent information should be retained only where it is necessary and proportionate to do so in accordance with the authorised purpose as set out in paragraph 8.5 or where otherwise required by law. It should be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there should be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised purpose.

8.30. Where confidential personal or constituent information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place.

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

Applications to acquire material relating to confidential journalistic material and journalists' sources

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

8.33. The acquisition of material through covert surveillance or property interference will be a justifiable interference with an individual's human rights under Articles 8 (right to respect for private and family life) and, in certain circumstances, 10 (freedom of expression) of the ECHR only if the conduct being authorised is necessary, proportionate and in accordance with law.

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

8.35. A person holds material in confidence if they hold the material subject to an express or implied undertaking to hold it in confidence, or they hold the material subject to a restriction on disclosure or an obligation of secrecy contained in an enactment. Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist nor the source (for example, a news editor who has been sent some notes by a journalist).

8.36. When a public authority applies for an authorisation where the purpose, or one of the purposes, of the authorisation is to authorise the acquisition of material that the authority believes will be confidential journalistic material, the authorisation application must contain a statement that the purpose is to acquire material which the public authority believes will contain confidential journalistic material. The person to whom the application is made may issue the authorisation only if they consider that appropriate safeguards relating to the handling, retention use and disclosure of the material are in place and where appropriate, Judicial Commissioner approval has been obtained.

8.37. A source of journalistic information is an individual who provides material intending the recipient to use it for the purpose of journalism or knowing that it is likely to be so used. Any reference to sources in this code should be understood to include any person acting as an intermediary between a journalist and a source.

8.38. When a public authority applies for an authorisation where the purpose, or one of the purposes is to identify or confirm a source of journalistic information, the application must contain a statement confirming that this is the purpose (or one of the purposes) for the application. The person to whom the application is made may issue the warrant or authorisation only if they consider that appropriate safeguards relating to the handling, retention, use and disclosure of the material are in place.

8.39. An assessment of whether someone is a journalist (for the purpose of this code) should be made on all the facts and circumstances available at the time. Consideration should be given, in particular, to the frequency of the individual's relevant activities, the level of personal rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the safeguards in this code, which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest. The fact that a person uses social media tools to communicate does not, in itself, indicate that that person is a journalist or that he or she is likely to be holding confidential journalistic material.

8.40. Where material is created or acquired with the intention of furthering a criminal purpose, the material is not to be regarded as having been created or acquired for the

purpose of journalism. Once material has been broadcast, no confidentiality can attach to the material so it is not confidential journalistic material.

8.41. Where confidential journalistic material, or that which identifies the source of journalistic information, is retained and disseminated to an outside body, reasonable steps should be taken to mark the disseminated information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of such information, advice should be sought from a legal adviser to the relevant public authority before any further dissemination of the content takes place.

8.42. Where confidential journalistic material, or that which identifies a source of journalistic information, has been obtained and retained, other than for the purposes of destruction, the matter should be reported to the IPC as soon as reasonably practicable.

Surveillance under the 2015 Order - Material subject to legal privilege

8.43. 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 affect 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.

8.44. 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.

8.45. 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.

8.46. 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.

8.47. 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.

8.48. 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.

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

8.50. 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.

8.51. 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 Judicial Commissioner; and

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

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

8.52. 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 likely or intending to obtain knowledge of matters subject to legal privilege.

8.53. 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, and approving Judicial Commissioner, as appropriate, are 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.

8.54. 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 Judicial Commissioner, as appropriate, 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.

8.55. 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.

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

The use and handling of matters subject to legal privilege

8.57. 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. The acquisition of knowledge of matters subject to legal privilege (whether deliberate or otherwise) is therefore subject to additional safeguards. These safeguards provide for three different circumstances.

i) Application process for covert surveillance or property interference likely to result in the acquisition of knowledge of matters subject to legal privilege

8.58. If the covert surveillance or property interference does not intend 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 clearly 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.

8.59. In addition, it should set out the reasons why the surveillance or interference with property is considered necessary and provide an assessment of how likely it is that information which is subject to legal privilege will be obtained. The relevant agency should also confirm that any collateral intrusion that is subject to legal privilege will be treated in accordance with the safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to the material that is subject to legal privilege.

8.60. Directed surveillance likely to result in the acquisition of knowledge of matters subject to legal privilege may be authorised only by authorising officers entitled to grant authorisations in respect of confidential information. Intrusive surveillance, including surveillance which is to be treated as intrusive by virtue of the 2015 Order, or property interference likely to result in the acquisition of material subject to legal privilege, may only

be authorised by authorising officers entitled to grant intrusive surveillance or property interference authorisations. Intrusive Surveillance and Property Interference authorisations shall not take effect unless approved by a Judicial Commissioner.

ii) Application process for covert surveillance or property interference intended to result in the acquisition of knowledge of matters subject to legal privilege

8.61. Where the intention is to acquire items subject to legal privilege, the application must contain a statement that the purpose, or one of the purposes, of the authorisation is to obtain legally privileged material. An authorisation should only be granted and approved if the authorising officer and Judicial Commissioner are satisfied that there are exceptional and compelling circumstances that make the authorisation necessary (see paragraph 8.54). The exceptional and compelling test can only be met when the public interest in obtaining the information sought outweighs the public interest in maintaining the confidentiality of legally privileged material, and when there are no other reasonable means of obtaining the required information. The authorised covert surveillance or property interference must be reasonably regarded as likely to yield the intelligence necessary to counter the threat.

8.62. Further, in considering any such application, the authorising officer and Judicial Commissioner must be satisfied that the proposed conduct is proportionate to what is sought to be achieved and must have regard to the public interest in the confidentiality of items subject to privilege. They will wish to consider carefully whether the activity or threat being investigated is of a sufficiently serious nature to override the public interest in preserving the confidentiality of privileged communications, and the likelihood that the information sought will have a positive impact on the investigation.

8.63. The authorising officer and Judicial Commissioner will take into account both the public interest in preserving the confidentiality of those particular items and the broader public interest in maintaining the confidentiality of items subject to legal privilege more generally. The authorising officer and Judicial Commissioner must be satisfied that there are appropriate arrangements in place for the handling, retention, use and destruction of privileged items. In such circumstances, the authorising officer and Judicial Commissioner will be able to impose additional requirements such as regular reporting arrangements so as to keep the authorisation under review more effectively.

iii) Application process for covert surveillance or property interference intended to result in the acquisition of knowledge of matters that would be subject to legal privilege if they were not created or held with the intention of furthering a criminal purpose

8.64. Where an application for an authorisation is made where the purpose, or one of the purposes, is to obtain items that, if they were not created or held with the intention of furthering a criminal purpose, would be subject to privilege and where the public authority considers that the items are likely to be created or held to further a criminal purpose, the application must include a statement to that effect and the reasons for believing that the items are likely to be created or held to further a criminal purpose. For example, if the public authority has reliable intelligence that a criminal fugitive is seeking advice from a lawyer in order to obtain a false alibi or to assist them in evading arrest, then this may provide grounds for an assessment that the communications with the lawyer will not be privileged, notwithstanding that the fugitive appeared to be seeking advice from a lawyer in a professional capacity, and this information should be set out in the application. The requirement to ensure the case for an authorisation is presented in the application in a fair

and balanced way, including information which supports or weakens the case for the warrant or authorisation (as set out in paragraph 4.36) applies in these circumstances as it does elsewhere. For example, information which may undermine the assessment that material is likely to be created or held to further a criminal purpose must also be included in the application to ensure the authorising officer and Judicial Commissioner can make an informed assessment about the nature of the material. The authorisation can only be issued where the authorising officer, or Judicial Commissioner if appropriate, considers that the items are likely to be created or held with the intention of furthering a criminal purpose.

8.65. Under the definition in the 1997 Act, legal privilege does not apply to communications or items held, or oral communications made, with the intention of furthering a criminal purpose. Privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

8.66. For the purposes of this code, any communication or items held between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the communication or item does not form part of a professional consultation of the lawyer, or there is clear and compelling evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the material is subject to legal privilege or over whether material is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from a legal adviser within the relevant public authority.

8.67. 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.

8.68. In cases likely to result in the acquisition of knowledge of matters subject to legal privilege, the authorising officer or Judicial 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 Judicial Commissioner or Inspector during his next inspection (at which the material should be made available if requested).

8.69. 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 Judicial Commissioner or Inspector during his next inspection and made available on request.

8.70. 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 Judicial Commissioner during his or her next inspection.

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

8.71. 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 Judicial Commissioner; and

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

Lawyers' material

8.72. Where a lawyer, acting in this professional capacity, is the subject of covert surveillance or property interference it is possible that a substantial proportion of the material which will be acquired will be subject to legal privilege. Therefore, in any case where the subject of covert surveillance or property interference is known to be a lawyer acting in that professional capacity, the application should be made on the basis that it is likely or intended to acquire items subject to legal privilege and the provisions in paragraphs 8.58 – 8.63 will apply, as relevant.

8.73. The public authority will wish to consider which of the three circumstances, which apply when items subject to legal privilege will or may be obtained, is relevant, and what processes should therefore be followed. This paragraph does not prevent an application being made on the grounds that the lawyer is under investigation for serious criminal offences, in which case, the application or notification must be made on the basis that it is likely to acquire items subject to legal privilege and the additional considerations set out at paragraphs 8.58 – 8.60 will apply.

8.74. Any case involving lawyers' material should also be notified to the IPC during his or her next inspection and any material which has been retained should be made available to the IPC on request.

Handling, retention, and deletion of legally privileged material

8.75. In addition to the general safeguards governing the handling and retention of material as provided for in paragraphs 8.14 – 8.21, authorised persons who analyse material obtained by covert surveillance or property interference should be alert to any communications or items which may be subject to legal privilege. Paragraphs 8.76 – 8.77 set out the additional arrangements that apply to legally privileged items where the intention is to retain them for a purpose other than their destruction.

8.76. A legal adviser to the public authority must be consulted when it is believed that material which attracts privilege is retained other than for the purpose of destruction. The legal adviser is responsible for determining that material is privileged rather than an officer who is involved in an investigation. In cases where there is doubt as to whether material is privileged or not, the IPC may be informed who will be able to give a view. Where it is discovered that privileged material has been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain it for one or more of the authorised purposes (see paragraph 8.5). If not, the material should not be retained, other than for the purpose of its destruction or in accordance with other statutory requirements.

8.77. Material which has been identified as legally privileged (and is being retained for purposes other than its destruction) should be clearly marked as subject to legal privilege and the IPC must be notified of the retention of the items as soon as reasonably practicable. Paragraphs 8.78 – 8.80 provides more detail on reporting privileged items to the IPC. Such material should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes. Privileged items must be securely destroyed when their retention is no longer needed for those purposes. If such material is retained, there must be adequate information management systems in place to ensure that continued retention, for purposes other than their destruction, remains necessary and proportionate for the authorised statutory purposes.

Reporting to the Investigatory Powers Commissioner

8.78. In those cases where items identified by a legal advisor in the public authority as being legally privileged have been acquired, the matter should be reported to the IPC as soon as reasonably practicable.

8.79. The IPC must order the destruction of the item or impose conditions on its use or retention unless the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. Even if retention is necessary and the public interest in its retention outweighs the public interest in the confidentiality of items subject to legal privilege, the IPC may still impose conditions as he considers necessary to protect the public interest in the confidentiality of items subject to privilege. It may be the case in some circumstances that privileged items can be retained when their retention does not outweigh the public interest in the confidentiality of items subject to privilege. This includes, for example, where it is not possible to separate privileged items from those that are not privileged and of intelligence value and where the retention is necessary and proportionate for one of more of the authorised purposes or in accordance with statutory requirements. In these circumstances, the IPC must impose conditions on the use or retention of the item.

8.80. The IPC will make an assessment of whether the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and of whether retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. If both of those conditions are met, then the IPC may impose conditions as to the use or retention of the items, but the IPC is not obliged to do so. If those conditions are not met, the IPC must direct that the item is destroyed, or must impose one or more conditions as to the use or retention of the items. The IPC must have regard to any representations made by the public authority about the proposed retention of privileged items or conditions that may be imposed.

Dissemination

8.81. In the course of an investigation, a public authority must not act on or further disseminate legally privileged items unless it has first informed the IPC that the items have been obtained, except in urgent circumstances. Where there is an urgent need to take action and it is not reasonably practicable to inform the IPC that the material has been obtained before taking action, the public authority may take action before informing the IPC. In such cases, the public authority should, wherever possible consult a legal adviser. A public authority must not disseminate privileged items if doing so would be contrary to a condition imposed by the IPC in relation to those items.

8.82. The dissemination of legally privileged material to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk 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, including law enforcement authorities. In this regard civil proceedings include all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Office and Procurator Fiscal Service lawyer nor any other prosecuting authority lawyer with conduct of a prosecution should have sight of any legally privileged material, held by the relevant public authority, with any possible connection to the proceedings. In respect of civil proceedings, there can be no circumstances under which it is proper for any public authority to have sight of or seek to rely on legally privileged material in order to gain a litigation advantage over another party in legal proceedings.

8.83. In order to safeguard against any risk of prejudice or accusation of abuse of process, public authorities must also take all reasonable steps to ensure that lawyers or other officials with conduct of legal proceedings should not see legally privileged material relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the public authority must seek independent advice from Counsel and, if there is assessed to be a risk that sight of such material could yield a litigation advantage, the direction of the Court must be sought.

DRAFT

9. Oversight

9.1. The IPA establishes an IPC, whose remit includes providing comprehensive oversight of the use of the powers to which this code applies, and adherence to the practices and processes described in it. By statute the IPC will be, or will have been, a member of the senior judiciary and will be entirely independent of the Scottish and UK Governments or any of the public authorities authorised to use investigatory powers. The IPC will be supported by inspectors and others, such as technical experts, qualified to assist the IPC in his or her work (the 'Technology Advisory Panel').

9.2. The IPC, and those that work under the authority of the IPC, will ensure compliance with the law and this code by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny.

9.3. The IPC will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the IPC must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers must, by law, offer all necessary assistance to the IPC and anyone who is acting on behalf of the IPC.

9.4. Anyone working for a public authority that has concerns about the way that investigatory powers are being used may report their concerns to the IPC, who will consider them. In particular, any person who exercises the powers to which this code applies should report to the IPC any action undertaken which they believe to be contrary to the provisions of this code. The IPC may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the IPT.

9.5. The IPC must report annually on the findings of their inspections and investigations. This report will be laid before the Scottish and UK Parliaments and will be made available to the public, subject to any necessary redactions made in the national interest. In relation to property interference, only the Prime Minister will be able to authorise redactions to the IPC's report, after consultation with the Scottish Ministers and the IPC. If the IPC disagrees with the proposed redactions to his or her report then the IPC may inform the Intelligence and Security Committee of the UK Parliament that they disagree with them.

9.6. In relation to covert surveillance, the IPC will report annually to the Scottish Ministers in respect of the carrying out of the Commissioner's functions and this report shall be laid before the Scottish Parliament. Any necessary redactions can only be made by the Scottish Ministers, after consultation with the IPC. The grounds for making a redaction are that the information would be contrary to the public interest or prejudicial to the prevention or detection of serious crime or the continued discharge of the functions of any public authority.

9.7. The IPC may also report, at any time, on any of their investigations and findings as they see fit. These reports will also be made publicly available subject to public interest considerations. Public authorities may seek general advice from the IPC on any issue which falls within the IPC's statutory remit. The IPC may also produce guidance for public authorities on how to apply and use investigatory powers. Wherever possible this guidance will be published in the interests of public transparency.

9.8. Further information about the IPC, their office and their work may be found at: [link to the website will be inserted once the IPC is established]

10. Complaints

10.1. The IPT has jurisdiction to investigate and determine complaints against public authority use of investigatory powers and human rights claims against the security and intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

10.2. The IPT is entirely independent from the Scottish and UK Governments and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination.

10.3. This code does not cover the exercise of the IPT's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: www.ipt-uk.com. Alternatively information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

10.4. If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

DRAFT

Annex A

Directed surveillance authorisation level when knowledge of confidential information is likely to be acquired

Relevant Public Authority	Authorisation level
The Police Service of Scotland	Chief Constable[48]
The Police Investigations and Review Commissioner	Commissioner
The Scottish Administration Marine Scotland	Head of Compliance
Accountant in Bankruptcy	Accountant in Bankruptcy
Scottish Prison Service	Chief Executive or Director of Operations
Contracted out prisons	Chief Executive or Director of Operations
Transport Scotland	Chief Executive
Food Standards Scotland	Chief Executive
A council constituted under section 2 of the Local Government etc (Scotland) Act 1994	Chief Executive
The Common Services Agency for the Scottish Health Service	Director of Practitioner and Counter Fraud Services
The Scottish Environment Protection Agency	Chief Executive

DRAFT

[48] Reference to the Chief Constable includes any other senior officer of the Police Service of Scotland who is designated by the Chief Constable for this purpose

© Crown copyright 2017

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit **nationalarchives.gov.uk/doc/open-government-licence/version/3** or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: **psi@nationalarchives.gsi.gov.uk**.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

Published by The Scottish Government, July 2017

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA

w w w . g o v . s c o t