APPENDIX 2

Home Office

Covert Surveillance and Property Interference

Code of Practice

Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000

December 2014

Home Office

Covert Surveillance and Property Interference

Code of Practice

Pursuant to section 71(4) of the Regulation of Investigatory Powers Act 2000

LONDON: TSO

TSO
information & publishing solutions

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries:
0870 600 5522
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

TSO@Blackwell and other Accredited Agents

Published with the permission of the Home Office on behalf of the Controller of Her Majesty's Stationery Office.

First published 2014

ISBN 9780113413737

Printed in the United Kingdom for The Stationery Office.
J002969998 C10 12/14

Contents

Chapter 1
INTRODUCTION

Definitions

1.1 In this code:

- '1989 Act' means the Security Service Act 1989;
- '1994 Act' means the Intelligence Services Act 1994;
- '1997 Act' means the Police Act 1997;
- '2000 Act' means the Regulation of Investigatory Powers Act 2000 (RIPA);
- 'RIP(S)A' means the Regulation of Investigatory Powers (Scotland) Act 2000;
- '2010 Order' means the Regulation of Investigatory powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010;
- terms in *italics* 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 Part II of the 2000 Act to authorise covert surveillance that is likely to result in the obtaining of *private information* about a person. The code also provides guidance on entry on, or interference with, property or with wireless telegraphy by *public authorities* under section 5 of the Intelligence Services Act 1994 or Part III of the Police Act 1997.

1.3 This code is issued pursuant to section 71 of the 2000 Act, which stipulates that the *Secretary of State* shall issue one or more codes of practice in relation to the powers and duties in Parts I to III of the 2000 Act, section 5 of the 1994 Act and Part III of the 1997 Act. This code replaces the previous code of practice issued in 2010.

1.4 This code is publicly available and should be readily accessible by *member*s of any relevant *public authority*[1] seeking to use the 2000 Act to authorise covert surveillance that is likely to result in the obtaining of *private information* about a person or section 5 of the 1994 Act or Part III of the 1997 Act to authorise entry on, or interference with, property or with wireless telegraphy.

1.5 Where covert surveillance activities are unlikely to result in the obtaining of *private information* about a person, or where there is a separate legal basis for such activities, neither the 2000 Act nor this code need apply.[2]

Effect of code

1.6 The 2000 Act provides that all codes of practice relating to the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under the 2000 Act, or to one of the Commissioners responsible for overseeing the powers conferred by the 2000 Act, it must be taken into account. *Public authorities* may also be required to justify, with regard to this code, the use or granting of *authorisations* in general or the failure to use or grant *authorisations* where appropriate.

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

---

1 Being those listed under section 30 of the 2000 Act or specified in orders made by the *Secretary of State* under that section.

2 See Chapter 2. It is assumed that intrusive surveillance will always result in the obtaining of *private information*.

Surveillance activity to which this code applies

1.8 Part II of the 2000 Act provides for the *authorisation* of covert surveillance by *public authorities* where that surveillance is likely to result in the obtaining of *private information* about a person.

1.9 Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.[3]

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

1.11 Specifically, covert surveillance may be authorised under the 2000 Act if it is either intrusive or directed:

- Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device);[5]
- Directed surveillance is covert surveillance that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of *private information* about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek *authorisation* under the 2000 Act).

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

3 See section 48(2) of the 2000 Act.

4 As defined in section 26(9)(a) of the 2000 Act.

5 See Chapter 2 for full definition of residential premises and private vehicles, and note that the 2010 Order identified a new category of surveillance to be treated as intrusive surveillance.

Basis for lawful surveillance activity

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

1.14 Part II of the 2000 Act provides a statutory framework under which covert surveillance activity can be authorised and conducted compatibly with Article 8. Where covert surveillance would not be likely to result in the obtaining of any *private information* about a person, no interference with Article 8 rights occurs and an *authorisation* under the 2000 Act is therefore not appropriate.

1.15 Similarly, an *authorisation* under the 2000 Act 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. For example the Police and Criminal Evidence Act 1984[6] provides a legal basis for the police covertly to record images of a suspect for the purposes of identification and obtaining certain evidence.

1.16 Chapter 2 of this code provides further guidance on what constitutes *private information* and examples of activity for which *authorisations* under Part II of the 2000 Act are or are not required.

6 See also the Police & Criminal Evidence (Northern Ireland) Order 1989.

Relevant public authorities

1.17 Only certain *public authorities* may apply for *authorisations* under the 2000, 1997 or 1994 Acts:

- Directed surveillance *applications* may only be made by those *public authorities* listed in or added to Part I and Part II of schedule 1 of the 2000 Act.
- Intrusive surveillance *applications* may only be made by those *public authorities* listed in or added to section 32(6) of the 2000 Act, or by those *public authorities* listed in or designated under section 41(1) of the 2000 Act.
- *Applications* to enter on, or interfere with, property or with wireless telegraphy may only be made (under Part III of the 1997 Act) by those *public authorities* listed in or added to section 93(5) of the 1997 Act; or (under section 5 of the 1994 Act) by the intelligence services.

Scotland

1.18 Where all the conduct authorised is likely to take place in Scotland, *authorisations* should be granted under RIP(S)A, unless:

- the *authorisation* is to be granted or renewed (by any relevant *public authority*) for the purposes of national security or the economic well-being of the UK;
- the *authorisation* is being obtained by, or authorises conduct by or on behalf of, those *public authorities* listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (*Authorisations* Extending to Scotland) Order 2000; SI No. 2418); or,
- the *authorisation* authorises conduct that is surveillance by virtue of section 48(4) of the 2000 Act.

1.19 This code of practice is extended to Scotland in relation to *authorisations* granted under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to *authorisations* granted under RIP(S)A.

International considerations

1.20 *Authorisations* under the 2000 Act can be given for surveillance both inside and outside the UK. However, *authorisations* for actions outside the UK can usually only validate them for the purposes of UK law. Where action in another country is contemplated, the laws of the relevant country must also be considered.

1.21 *Public authorities* are therefore advised to seek *authorisations* under the 2000 Act for directed or intrusive surveillance operations outside the UK if the subject of investigation is a UK national or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court.

1.22 *Authorisations* under the 2000 Act are appropriate for all directed and intrusive surveillance operations in overseas areas under the jurisdiction of the UK, such as UK Embassies, military bases and detention facilities.

1.23 Under the provisions of section 76A of the 2000 Act, 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.

Chapter 2
DIRECTED AND INTRUSIVE SURVEILLANCE DEFINITIONS

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

Directed surveillance

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

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of *private information* about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an *authorisation* under Part II of the 2000 Act to be sought.

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

Private information

2.4 The 2000 Act states that *private information* includes any information relating to a person's private or family life.[7] *Private information* should be taken generally to include any aspect of a person's private or personal relationship with others, including family[8] and professional or business relationships.

2.5 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of *private information*. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a *public authority* of that person's activities for future consideration or analysis.[9]

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.

2.6 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances,

7 See section 26(10) of the 2000 Act.

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.

the totality of information gleaned may constitute *private information* even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance *authorisation* may be considered appropriate.

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

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

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.

Specific situations requiring directed surveillance authorisations

2.8 The following specific situations may also constitute directed surveillance according to the 2000 Act:

- The use of surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle alone does not necessarily constitute directed surveillance as they do not necessarily provide *private information* about any individual but sometimes only supply information about the location of that particular device at any one time. However, the use of that information, when coupled with other surveillance activity which may obtain *private information*, could interfere with Article 8 rights. A directed surveillance *authorisation* may therefore be appropriate.[11]
- Surveillance consisting of the interception of a communication in the course of its transmission by means of a public postal service or telecommunication system where the communication is one sent or intended for a person who has consented to the interception of communications sent by or to them and where there is no interception *warrant*[12] authorising the interception.[13]

Recording of telephone conversations

2.9 Subject to paragraph 2.8 above, the interception of communications sent by public post or by means of public telecommunications systems or private telecommunications is governed by Part I of the 2000 Act. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the 2000 Act.

11 The use of such devices is also likely to require an *authorisation* for property interference under the 1994 or 1997 Act. See Chapter 7.

12 i.e. under Part 1 Chapter 1 of the 2000 Act.

13 See section 48(4) of the 2000 Act. The availability of a directed surveillance *authorisation* nevertheless does not preclude authorities from seeking an interception *warrant* under Part I of the 2000 Act in these circumstances.

2.10 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 I of the 2000 Act provided the process by which the product is obtained does not involve any modification of, or interference with, the telecommunications system or its operation. This will not constitute interception as sound waves obtained from the air are not in the course of transmission by means of a telecommunications system (which, in the case of a telephone conversation, should be taken to begin with the microphone and end with the speaker). Any such product can be treated as having been lawfully obtained.

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

Intrusive surveillance

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

2.12 The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained. In addition, directed surveillance under the ambit of the 2010 Order is to be treated as

intrusive surveillance. Accordingly, it is not necessary to consider whether or not intrusive surveillance is likely to result in the obtaining of *private information*.

Residential premises

2.13 For the purposes of the 2000 Act, 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]

2.14 The 2000 Act further states that the concept of premises should be taken to include any place whatsoever, including any vehicle or moveable structure, whether or not occupied as land.

2.15 Examples of residential premises would therefore include:

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

2.16 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;

14 See section 48(1) of the 2000 Act.

15 See section 48(7) of the 2000 Act.

- residential premises occupied by a *public authority* for non-residential purposes; for example, trading standards 'house of horrors' situations or undercover operational premises.

Private vehicles

2.17 A private vehicle is defined in the 2000 Act 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.[16]

Places for legal consultation

2.18 The 2010 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 Part II of the 2000 Act as intrusive surveillance. The premises identified in Article 3(2) are:

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

(b) any place 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 Border Act 2007;

(c) police stations;

(d) hospitals where high security psychiatric services are provided;

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

(f) any place used for the sittings and business of any court, tribunal, inquest or inquiry.

16 See section 48(1) and 48 (7) of the 2000 Act.

Further considerations

2.19 Intrusive surveillance (or directed surveillance being treated as intrusive surveillance under the 2010 Order) may take place by means of a person or device located in residential premises or a private vehicle or 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.[17]

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

2.20 The use of a device for the purpose of providing information about the location of any private vehicle is not considered to be intrusive surveillance.[18] Such use may, however, be authorised as directed surveillance, where the recording or use of the information would amount to the covert monitoring of the movements of the occupant(s) of that vehicle. A property interference *authorisation* may be appropriate for the covert installation or deployment of the device.

Where authorisation is not required

2.21 Some surveillance activity does not constitute intrusive or directed surveillance for the purposes of Part II of the 2000 Act and no directed or intrusive surveillance *authorisation* can be provided for such activity. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to specified grounds;

17 See section 26(5) of the 2000 Act.

18 See section 26(4) of the 2000 Act.

- overt use of CCTV and ANPR systems;[19]
- certain other specific situations.

2.22 Each situation is detailed and illustrated below.

Immediate response

2.23 Covert surveillance that is likely to reveal *private information* about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an *authorisation* under the 2000 Act, would not require a directed surveillance *authorisation*. The 2000 Act is not intended to prevent law enforcement *officer*s fulfilling their legislative functions. To this end section 26(2)(c) of the 2000 Act 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 the 2000 Act would not be appropriate where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol.

General observation activities

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

19 See the Surveillance Camera Code of Practice issued under Part 2 of the Protection of Freedoms Act 2012 for guidance on the overt use of surveillance cameras, including CCTV and ANPR in public places. This applies in England and Wales.

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

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

Example 3: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A trained employee or person engaged by a public authority is deployed to act as a juvenile in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the Act, that a public authority may conclude that a covert human intelligence source (CHIS) authorisation is unnecessary. However, if the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation.

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 therefore be considered.

Surveillance not relating to specified grounds or core functions

2.25 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 28(3) of the 2000 Act. Covert surveillance for any other general purposes should be conducted under other legislation, if relevant, and an *authorisation* under Part II of the 2000 Act should not be sought.

2.26 The 'core functions' 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.). A *public authority* may only engage the 2000 Act when in performance of its 'core functions'. The disciplining of an employee is not a 'core function', although related criminal investigations may be. The protection of the 2000 Act 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 his employer of undertaking additional employment in breach of discipline regulations. The police force of which he is a member 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 the 2000 Act as it does not relate to the discharge of the police force'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.

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

CCTV and automatic number plate recognition (ANPR) cameras

2.27 The use of overt CCTV cameras by *public authorities* does not normally require an *authorisation* under the 2000 Act. Members of the public should be made aware that such systems are in use. For example, by virtue of cameras or signage being clearly visible, through the provision of information and by undertaking consultation. Guidance on their operation is provided in the

Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012. This sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the Data Protection Act 1998 and a public authority's duty to adhere to the Human Rights Act 1998. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an *authorisation* under the 2000 Act.

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

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

Example: A local police team receive information that an individual suspected of committing thefts from motor vehicles is known to be in a town centre area. A decision is taken to use the town centre CCTV system to conduct surveillance against that individual such that 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.

Online covert activity

2.29 The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

Specific situations not requiring authorisation

2.30 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 them to record any information obtained in their presence;[20]

20 See section 48(3) of the 2000 Act.

- 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;
- the covert recording of noise where: the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm) or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an *authorisation* is unlikely to be required;
- the use of apparatus outside any residential or other premises exclusively for the purpose of detecting the installation or use of a television receiver within those premises. The Regulation of Investigatory Powers (British Broadcasting Corporation) Order 2001 (SI No. 1057) permits the British Broadcasting Corporation to authorise the use of apparatus for this purpose under Part II of the 2000 Act, although such use constitutes neither directed nor intrusive surveillance;[21]
- entry on or interference with property or wireless telegraphy under section 5 of the 1994 Act or Part III of the 1997 Act (such activity may be conducted in support of surveillance, but is not in itself surveillance).[22]

21 See section 26(6) of the 2000 Act.

22 See section 48(3) of the 2000 Act.

Chapter 3
GENERAL RULES ON AUTHORISATIONS

Overview

3.1 An *authorisation* under Part II of the 2000 Act 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 section 5 of the 1994 Act or Part III of the 1997 Act will provide lawful authority for *member*s of the intelligence services, police, National Crime Agency (NCA) or Her Majesty's Revenue and Customs (HMRC) to enter on, or interfere with, property or wireless telegraphy.

3.2 Responsibility for granting *authorisations* varies depending on the nature of the operation and the *public authority* involved. The relevant *public authorities* and *authorising officers* are detailed in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

Necessity and proportionality

3.3 The 2000 Act, 1997 Act and 1994 Act stipulate that the person granting an *authorisation* or *warrant* for directed or intrusive surveillance, or interference with property, must believe that the activities to be authorised are necessary on one or more statutory grounds.[23]

23 These statutory grounds are laid out in sections 28(3) of the 2000 Act for directed surveillance; section 32(3) of the 2000 Act for intrusive surveillance; and section 93(2) of the 1997 Act and section 5 of the 1994 Act for property interference. They are detailed in Chapters 5, 6 and 7 for directed surveillance, intrusive surveillance and interference with property respectively.

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

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

3.6 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

3.7 It is important therefore that all those involved in undertaking directed or intrusive surveillance activities or interference with property under the 2000 Act, 1997 Act or 1994 Act are fully aware of the extent and limits of the *authorisation* or *warrant* in question.

Example: 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.

Collateral intrusion

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

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

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

Example: HMRC seeks to conduct directed surveillance against T on the grounds that this is necessary and proportionate for the collection of a tax. It is assessed that such surveillance will unavoidably result in the obtaining of some information about members of T's family, who are not the intended subjects of the surveillance. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation. This may include not recording or retaining any material obtained through such collateral intrusion.

3.11 Where it is proposed to conduct surveillance activity or property interference specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such surveillance or property interference activity should be carefully considered against the necessity and proportionality criteria as described above (paragraphs 3.3–3.8).

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

Combined authorisations

3.12 A single *authorisation* may combine:

- any number of *authorisations* under Part II of the 2000 Act;[24]
- an *authorisation* under Part II of the 2000 Act[25] and an *authorisation* under Part III of the 1997 Act;
- a *warrant* for intrusive surveillance under Part II of the 2000 Act[26] and a *warrant* under section 5 of the 1994 Act.

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

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

Collaborative working

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

---

24 See section 43(2) of the 2000 Act.

25 On the *application* of a *member* of a police force, NCA, a customs *officer* or an *officer* of the CMA. See section 33(5) of the 2000 Act.

26 On the *application* of a *member* of the intelligence services. See section 42(2) of the 2000 Act.

3.16 In cases where one agency or force is acting on behalf of another, the tasking agency should normally obtain or provide the *authorisation* under Part II of the 2000 Act. For example, where surveillance is carried out by the police on behalf of HMRC, *authorisations* would usually be sought by HMRC and granted by the appropriate *authorising officer*. Where the operational support of other agencies (in this example, the police) is foreseen, this should be specified in the *authorisation*.

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

3.18 Where an individual or a non-governmental organisation is acting under direction of a public authority then they are acting as an agent of that public authority and any activities they conduct which meet the 2000 Act definitions of directed or intrusive surveillance or amount to property interference for the purposes of the 1994 or 1997 Act, should be considered for authorisation under those Acts.

3.19 There are three further important considerations with regard to collaborative working:

3.20 NCA and HMRC *applications* for directed or intrusive surveillance and property interference, and Competition and Markets Authority (CMA) *applications* for intrusive surveillance, must only be made by a *member* or *officer* of the same force or agency as the *authorising officer*, regardless of which force or agency is to conduct the activity.

3.21 Police *applications* for directed or intrusive surveillance and property interference must only be made by a *member* or *officer* of the same force as the *authorising officer*, unless the Chief *Officer*s of the forces in question have made a collaboration agreement under the Police Act 1996 and the collaboration agreement permits applicants and *authorising officers* to be from different forces.

3.22 *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 the area of operation of the force or agency applying for the *authorisation*. This requirement does not apply where the Chief *Officers* of two or more police forces have made a collaboration agreement under the Police Act 1996 and the collaboration agreement permits *authorising officers* to authorise conduct in relation to premises or property in the force areas of forces other than their own which are party to the agreement.

Reviewing authorisations

3.23 Regular reviews of all *authorisations* should be undertaken to assess the need for the surveillance or property interference activity to continue. The results of a review should be retained for at least three years (see Chapter 8). Particular attention is drawn to the need to review *authorisations* frequently where the surveillance or property interference involves a high level of intrusion into private life or significant collateral intrusion, or *confidential information* is likely to be obtained.

3.24 In each case the frequency of reviews should be considered at the outset by the *authorising officer* or, for those subject to *authorisation* by the *Secretary of State*, the *member* or *officer* who made the *application* within the *public authority* concerned. This should be as frequently as is considered necessary and practicable.

3.25 In some cases it may be appropriate for an *authorising officer* to delegate the responsibility for conducting any reviews to a subordinate *officer*. The *authorising officer* is, however, 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.

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

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

General best practices

3.28 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;[27]
- where *authorisations* are granted orally under urgency procedures (see Chapters 5, 6 and 7 on *authorisation* procedures), a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the *applicant* and *authorising officer* as a priority. There is then no requirement subsequently to submit a full written *application*;
- an *application* should not require the sanction of any person in a *public authority* other than the *authorising officer*;
- where it is foreseen that other agencies will be involved in carrying out the surveillance, these agencies should be detailed in the *application*;
- *authorisations* should not generally be sought for activities already authorised following an *application* by the same or a different *public authority*.

3.29 Furthermore, it is considered good practice that within every relevant *public authority*, a senior responsible *officer*[28] 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 Part II of the 2000 Act, Part III of the 1997 Act and with this code;
- engagement with the Commissioners and inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

27 As laid out in Chapters 5, 6 and 7 of this code.

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

Local authorities

3.30 The Protection of Freedoms Act 2012 amended the 2000 Act to make local authority authorisations subject to judicial approval. The change means that local authorities need to obtain an order approving the grant or renewal of an authorisation from a judicial authority, before it can take effect. In England and Wales an application for such an Order must be made to a Justice of the Peace (JP). If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he or she will issue an order approving the grant or renewal for the use of the technique as described in the application. The amendment means that local authorities are no longer able to orally authorise the use of RIPA techniques. All authorisations must be made in writing and require JP approval. The authorisation cannot commence until this has been obtained.

3.31 In Scotland this requirement only applies to authorisations for communications data as the use of the other techniques is governed by RIP(S)A. Where such an authorisation is required by a local authority in Scotland, an application for grant or renewal should be made to a sheriff. For other activities/authorisations, local authorities in Scotland should refer to devolved legislation. In Northern Ireland this requirement only applies to authorisations where the grant or renewal relates to a Northern Ireland excepted or reserved matter. Where such an authorisation is required by a local authority in Northern Ireland, an application for a grant or renewal should be made to a district judge. For other authorisations, local authorities in Northern Ireland should refer to the general requirements for authorisation set out in this code.

3.32 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 has the following effects:

- Local authorities in England and Wales can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least six months'

imprisonment **or** are related to the underage sale of alcohol and tobacco. The offences relating to the latter are in Article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

- Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least six months' imprisonment.
- Local authorities may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.
- Local authorities may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a JP has been granted.
- A local authority **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting.

3.33 The provisions of the Order, detailed above, do not apply to Scotland and Northern Ireland.

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

3.35 Elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

Chapter 4
LEGALLY PRIVILEGED AND CONFIDENTIAL INFORMATION

Overview

4.1 The 2000 Act does not provide any special protection for '*confidential information*', although the 1997 Act makes special provision for certain categories of *confidential information*. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where *confidential information* is involved. *Confidential information* consists of communications subject to *legal privilege*, communications between a *Member of Parliament* and another person on constituency matters, confidential personal information, or confidential journalistic material. So, for example, extra care should be taken where, by undertaking surveillance of an individual it is likely that knowledge will be acquired of communications between a minister of religion and that individual relating to the latter's spiritual welfare, or between a *Member of Parliament* and that individual where he or she is a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality or *legal privilege* may be involved.

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

4.3 *Authorisation*s for directed surveillance of legal consultations falling within the 2010 Order, must comply with the enhanced *authorisation* regime described below. In cases where it is likely that knowledge of *confidential information* will be acquired, the use of covert

surveillance is subject to a higher level of *authorisation* e.g. a Chief *Officer*. Annex A lists the *authorising officer* for each *public authority* permitted to authorise such surveillance.

Material subject to legal privilege: introduction

4.4 Covert 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 2010 Order or in other circumstances. Similarly, property interference may be necessary in order to effect surveillance described in the same Order, or in other circumstances where knowledge of matters subject to *legal privilege* is likely to be obtained.

4.5 The 2010 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 Part II of the 2000 Act as intrusive surveillance.

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

(a) a consultation between a professional legal adviser and his client or any person representing his client, or

(b) a consultation between a professional legal adviser or his client or any such representative and a medical practitioner made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

4.7 The definition of 'legal consultation' in the 2010 Order, does not distinguish between legal consultations which are legally privileged, wholly or in part, and legal consultations which may be in furtherance of a criminal purpose are therefore not protected by *legal privilege*. Covert surveillance of all legal consultations covered by the 2010 Order (whether protected by *legal privilege* or not) is to be treated as intrusive surveillance.

4.8 '*Legal privilege*' is defined in section 98 of the 1997 Act. This definition should be used to determine how to handle material obtained through surveillance authorised under RIPA, including through surveillance which is treated as intrusive surveillance as a result of the 2010 Order. As discussed below, special safeguards apply to matters subject to *legal privilege*.

4.9 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 (whether the lawyer is acting unwittingly or culpably). Legally privileged communications or items will lose their protection for these other purposes if the professional legal adviser intends to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence.

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

4.10 All *application*s for covert surveillance or property interference that may result in the acquisition of knowledge of matters subject to *legal privilege* should state whether the covert surveillance or property interference is intended to obtain knowledge of matters subject to *legal privilege* as defined by section 98 of the 1997 Act.

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

4.12 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*, *Secretary of State* or approving Surveillance Commissioner, as appropriate, is satisfied that there are exceptional and compelling circumstances that make the *authorisation* necessary:

- Where the surveillance or property interference is not intended to result in the acquisition of knowledge of matters subject to *legal privilege*, such exceptional and compelling circumstances may arise in the interests of national security or the economic well-being of the UK, or for the purpose 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, or to national security, and the surveillance or property interference is reasonably regarded as likely to yield intelligence necessary to counter the threat.

4.13 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*, *Secretary of State* or approving Surveillance 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 2010 Order, section 32(4) will apply.

4.14 Directed surveillance likely to result in the acquisition of knowledge of matters subject to *legal privilege* may be authorised only by *authorising officer*s entitled to grant *authorisation*s in respect of *confidential information*. Intrusive surveillance, including surveillance which is treated as intrusive by virtue of the 2010 Order, or property interference likely to result in the acquisition of material subject to *legal privilege* may only be authorised by *authorising officer*s entitled to grant intrusive surveillance or property interference *authorisation*s.

4.15 Property interference likely to result in the acquisition of such material is subject to prior approval by a Surveillance Commissioner (unless the *Secretary of State* is the relevant *authorising officer* or the case is urgent). Intrusive surveillance, including surveillance which is treated as intrusive by virtue of the 2010 Order is subject to prior approval by a Surveillance Commissioner (unless the *Secretary of State* is the relevant *authorising officer* or the case is urgent).

Surveillance under the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010

4.16 As noted above, the 2010 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 Part II of the 2000 Act as intrusive surveillance.

4.17 As a result of the 2010 Order, such surveillance cannot be undertaken without the prior approval of a Surveillance Commissioner (with the exception of urgent *authorisations* or *authorisations* granted by the *Secretary of State*).

4.18 The locations specified in the Order are:

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

(b) any place 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 Border Act 2007;

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

(d) police stations;

(e) the place of business of any professional legal adviser;

(f) any place used for the sittings and business of any court, tribunal, inquest or inquiry.

4.19 With the exception of urgent *applications* and *authorisations* granted by the *Secretary of State*, *authorisations* for surveillance which is to be treated as intrusive surveillance as a result of the 2010 Order shall not take effect until such time as:

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

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

4.20 If an *authorisation* is to be granted by the *Secretary of State*, the provisions in Chapter 6 apply.

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

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

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

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

The use and handling of matters subject to legal privilege

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

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

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

4.25 A substantial proportion of the communications between a lawyer and his or her client(s) may be subject to *legal privilege*. Therefore, in any case where a lawyer is the subject of an investigation or operation, *authorising officer*s 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 relevant Commissioner or Inspector during his or her next inspection and made available on request.

4.26 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 subject to *legal privilege* due to the 'in furtherance of a criminal purpose' exception. The retention of legally privileged material, or its dissemination 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 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 legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during his or her next inspection.

Confidential information

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

4.28 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it.[29] Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples include consultations between a health professional and a patient, or information from a patient's medical records.

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

4.30 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.

---

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

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

Chapter 5
AUTHORISATION PROCEDURES FOR DIRECTED SURVEILLANCE

Authorisation criteria

5.1 Under section 28(3) of the 2000 Act an *authorisation* for directed surveillance may be granted by an *authorising officer* where he or she believes that the *authorisation* is necessary in the circumstances of the particular case on the grounds that it is:

(a) in the interests of national security;[30,31]

(b) for the purpose of preventing or detecting[32] crime or of preventing disorder;

(c) in the interests of the economic well-being of the UK;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;[33]

---

30 One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. An *authorising officer* in another *public authority* shall not issue a directed surveillance *authorisation* under Part II of the 2000 Act where the investigation or operation falls within the responsibilities of the Security Service, as set out above, except where the investigation or operation is to be carried out by a Special Branch or other police unit with formal counter-terrorism responsibilities (such as Counter Terrorism Units, Counter Terrorism Intelligence Units and Counter Terrorism Command) or where the Security Service has agreed that another *public authority* can carry out a directed surveillance investigation or operation which would fall within the responsibilities of the Security Service.

31 HM Forces may also undertake operations in connection with a military threat to national security and other operations in connection with national security in support of the Security Service, the Police Service of Northern Ireland or other Civil Powers.

32 Detecting crime is defined in section 81(5) of the 2000 Act 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.

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

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;[34] or

(g) for any other purpose prescribed by an order made by the *Secretary of State*.[35]

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

Relevant public authorities

5.3 The *public authorities* entitled to authorise directed surveillance (including to acquire *confidential information*, with specified higher *authorisation*), are listed in Schedule 1 to the 2000 Act. The specific purposes for which each *public authority* may obtain a directed surveillance *authorisation* are laid out in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

Authorisation procedures

5.4 Responsibility for authorising the carrying out of directed surveillance rests with the *authorising officer* and requires the personal authority of the *authorising officer*. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 designates the *authorising officer* for each different *public authority* and the *officer*s entitled to act in urgent cases. Where an *authorisation* for directed surveillance is combined with a *Secretary of State authorisation* for intrusive surveillance, the combined *authorisation* must be issued by the *Secretary of State*.

5.5 An *authorising officer* must give *authorisations* in writing, except that in urgent cases they may be given orally by the *authorising officer* or in writing by the *officer* entitled to act in urgent cases. In such cases, a record that the *authorising officer* has expressly authorised the action

34 This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

35 This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

should be recorded in writing by both the *authorising officer* and the applicant as soon as is reasonably practicable, together with the information detailed below.

5.6 A case is not normally to be regarded as urgent unless the time that would elapse before the *authorising officer* was available to grant the *authorisation* would, in the judgement of the person giving the *authorisation*, be likely to endanger life or jeopardise the investigation or operation for which the *authorisation* was being given. An *authorisation* is not 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.

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

Information to be provided in applications for authorisation

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

- the reasons why the *authorisation* is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in section 28(3) of the 2000 Act;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- a summary of the intelligence case and appropriate unique intelligence references where applicable;

- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any *confidential information* that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- 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.

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

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

Duration of authorisations

5.10 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 was granted.

5.11 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* was granted.

Renewals

5.12 If, at any time before an *authorisation* for directed surveillance granted by a *member* of the intelligence services would cease to have effect, a *member* of the intelligence services who is entitled to grant such *authorisations* considers that it is necessary for the *authorisation* to continue on the grounds of national security or in the interests of the economic well-being of the UK, he or she may renew it for a further period of six months, beginning with the day on which it would have ceased to have effect but for the renewal.

5.13 If, at any time before any other 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 or she 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.

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

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

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

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

Cancellations

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

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

Foreign surveillance teams operating in UK

5.19 The provisions of section 76A of the 2000 Act as inserted by the Crime (International Co-Operation) Act 2003 provide for foreign surveillance teams to operate in the UK, subject to the following procedures and conditions.

5.20 Where a foreign police or customs officer, who is conducting directed or intrusive surveillance activity outside the UK, needs to enter the UK for the purposes of continuing that surveillance, and

where it is not reasonably practicable for a UK officer to carry out the surveillance under the authorisation of Part II of the 2000 Act (or of RIP(S)A), the foreign officer must notify a person designated by the Director General of NCA immediately after entry to the UK and shall request (if this has not been done already) that an application for authorisation of such surveillance be made under Part II of the 2000 Act (or RIP(S)A 2000).

5.21 The foreign officer may then continue to conduct 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 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 the 2000 Act.

Chapter 6
AUTHORISATION PROCEDURES FOR INTRUSIVE SURVEILLANCE

General authorisation criteria

6.1 An *authorisation* for intrusive surveillance may be granted by the *Secretary of State* – for *applications* by the intelligence services, the Ministry of Defence or HM Forces[36] – or by a *senior authorising officer* or designated deputy of the police, NCA, HMRC or CMA, as listed in section 32(6) and 34(6) of the 2000 Act.

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 above, on combined *authorisations*).

6.3 Under section 32(2), (3) and (3A) of the 2000 Act the *Secretary of State* or the *senior authorising officer* or designated deputy may only authorise intrusive surveillance if they believe:

(a) that the *authorisation* is necessary in the circumstances of the particular case on the grounds that it is:

– in the interests of national security;[37]

36 Or any other *public authority* designated for this purpose under section 41(1) of the 2000 Act.

37 A *senior authorising officer* or designated deputy of a law enforcement agency shall not issue an *authorisation* for intrusive surveillance where the investigation or operation is within the responsibilities of one of the intelligence services and properly falls to be authorised by *warrant* issued by the *Secretary of State* under Part II of the 2000 Act or the 1994 Act.

– for the purpose of preventing or detecting serious crime;[38]
– in the interests of the economic well-being of the UK; or
– (in the case of the CMA) for the purpose of preventing or detecting an offence under section 188 of the Enterprise Act 2002 (cartel offence);

and

(b) that the surveillance is proportionate to what is sought to be achieved by carrying it out.

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.

Authorisation procedures for the police, NCA, HMRC and CMA – senior authorising officers and designated deputies

6.5 The *senior authorising officers* for these bodies are listed in section 32(6) of the 2000 Act. If the *senior authorising officer* is absent[39] then, under section 34(2) of the 2000 Act, an *authorisation* can be given by the designated deputy as provided for in section 12A of the Police Act 1996, section 18 of the Police and Fire Reform (Scotland) Act 2012 and section 25 of the City of London Police Act 1839.

38 Serious crime is defined in section 81(2) and (3) as crime that comprises an offence for which a person who has attained the age of 21 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.

39 The consideration of an *authorisation* by the *senior authorising officer* is only to be regarded as not reasonably practicable (within the meaning of section 34(2) of the 2000 Act) if he or she is on annual leave, is absent from the office and home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine. Pressure of work is not normally to be regarded as rendering it impracticable for a *senior authorising officer* to consider an *application*. Where a designated deputy gives an *authorisation* this should be made clear and the reason for the absence of the *senior authorising officer* given.

Urgent cases

6.6 The *senior authorising officer* or designated deputy should generally give *authorisations* in writing. However, in urgent cases, oral *authorisations* may be given by the *senior authorising officer* or designated deputy. 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 below.

6.7 In an urgent case, where it is not reasonably practicable having regard to the urgency of the case for either the *senior authorising officer* or the designated deputy to consider the *application*, an *authorisation* may be granted in writing by a person entitled to act only in urgent cases under section 34(4) of the 2000 Act.[40]

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.

Jurisdictional considerations

6.9 A police or NCA *authorisation* cannot be granted unless the *application* is made by a *member* of the same force or agency, unless, in the case of the police, a relevant collaboration agreement has been made (see above, on collaborative working). An HMRC or CMA *authorisation* cannot be granted unless the *application* is made by an *officer* of Revenue and Customs or CMA respectively.

40 Note that out-of-hours *officers* of assistant chief constable rank or above will be entitled to act for this purpose.

6.10 Where the surveillance is carried out in relation to any residential premises, the *authorisation* cannot be granted unless the residential premises are in the same area of operation of the force or organisation, unless, in the case of the police, a relevant collaboration agreement has been made (see above, on collaborative working).

Approval of Surveillance Commissioners

6.11 Except in urgent cases a police, NCA, HMRC or CMA *authorisation* granted for intrusive surveillance will not take effect until it has been approved by a Surveillance Commissioner and written notice of the 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 force or organisation.

6.12 When the *authorisation* is urgent it will take effect from the time it is granted provided notice is given to the Surveillance Commissioner in accordance with section 35(3)(b) (see section 36(3) of the 2000 Act).

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

Notifications to Surveillance Commissioners

6.14 Where a person grants, renews or cancels an *authorisation* for intrusive surveillance, he or she must, as soon as is reasonably practicable, give notice in writing to a Surveillance Commissioner, where relevant, in accordance with whatever arrangements have been made by the Chief Surveillance Commissioner.[41]

41 The information to be included in the notification to the Surveillance Commissioner is set out in the Regulation of Investigatory Powers (Notification of *Authorisations* etc.) Order 2000; SI No. 2563.

6.15 In urgent cases, the notification must specify the grounds on which the case is believed to be one of urgency. The urgency provisions should not be used routinely. If the Surveillance Commissioner is satisfied that there were no grounds for believing the case to be one of urgency, he or she has the power to quash the *authorisation*.

Authorisation procedures for Secretary of State authorisations

6.16 Intrusive surveillance by any of the intelligence services, the Ministry of Defence or HM Forces[42] requires the approval of a *Secretary of State*, unless these bodies are acting on behalf of another *public authority* that has obtained an *authorisation*.

6.17 Any *member* or official of the intelligence services, the Ministry of Defence and HM Forces can apply to the *Secretary of State* for an intrusive surveillance *authorisation*. *Applications* to the *Secretary of State* should specify those matters listed below.

6.18 Intelligence services *authorisations* must be made by issue of a *warrant*. Such *warrant*s will generally be given in writing by the *Secretary of State*. In urgent cases, a *warrant* may be signed (but not renewed) by a senior official, with the express *authorisation* of the *Secretary of State*.

Information to be provided in all applications for intrusive surveillance

6.19 *Applications* should be in writing (unless urgent) 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 (e.g. for the purpose of preventing or detecting serious crime) listed in section 32(3) of the 2000 Act;
- the nature of the surveillance;

42 Or any other *public authority* designated for this purpose under section 41(1) of the 2000 Act, such as the Home Office on the *application* of a *member* of HM Prison Service (SI 1126; 2001).

- 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;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- a record should be made of whether the *authorisation* was given or refused, by whom and the time and date at which this happened.

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

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

Duration of intrusive surveillance authorisations – Secretary of State warrants for the intelligence services

6.21 A *warrant* issued by the *Secretary of State* will cease to have effect at the end of a period of six months beginning with the day on which it was issued. So an *authorisation* given at 09.00 on 12 February will expire on 11 August. (*Authorisations* (except those granted under urgency provisions) will cease at 23.59 on the last day).

6.22 *Warrant*s expressly authorised by a *Secretary of State*, but signed by a senior official under the urgency procedures, will cease to have effect at the end of the second working day following the day of issue of the *warrant* unless renewed by the *Secretary of State*.

Duration of intrusive surveillance authorisations – all other intrusive surveillance authorisations

6.23 A written *authorisation* granted by a *Secretary of State*, a *senior authorising officer* or a designated deputy 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).

6.24 Oral *authorisations* given in urgent cases by a *Secretary of State*, a *senior authorising officer* or designated deputy, 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 – Secretary of State authorisations

6.25 If at any time before an intelligence service *warrant* expires, the *Secretary of State* considers it necessary for the *warrant* to be renewed for the purpose for which it was issued, the *Secretary of State* may renew it in writing for a further period of six months, beginning with the day on which it would have ceased to have effect, but for the renewal.

6.26 If at any time before a *warrant* issued by a *Secretary of State* for any other *public authority* expires, the *Secretary of State* considers it necessary for the *warrant* to be renewed for the purpose for which it was issued, he or she may renew it in writing for a further period of three months, beginning with the day on which it would have ceased to have effect, but for the renewal.

Renewals of intrusive surveillance authorisations – all other intrusive surveillance authorisations

6.27 If, at any time before an *authorisation* expires, the *senior authorising officer* or, in their absence, the designated deputy considers that the *authorisation* should continue to have effect for the purpose for which it was issued, he or she may renew it in writing for a further period of three months.

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

6.29 In urgent cases, a renewal can take effect immediately (provided this is not before the day on which the *authorisation* would have otherwise ceased to have effect). See section 35 and 36 of the 2000 Act and the Regulation of Investigatory Powers (Notification of *Authorisations* etc.) Order 2000; SI No. 2563.

Information to be provided for all renewals of intrusive surveillance authorisations

6.30 All *applications* for a renewal of an intrusive surveillance *authorisation* or *warrant* should record:

- whether this is the first renewal or every occasion on which the *warrant/authorisation* has been renewed previously;
- any significant changes to the information listed in paragraph 6.19;
- the reasons why it is necessary to continue with the intrusive surveillance;
- the content and value to the investigation or operation of the product so far obtained by the surveillance;
- the results of any reviews of the investigation or operation (see below).

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

Cancellations of intrusive surveillance activity

6.32 The *senior authorising officer* who granted or last renewed the *authorisation* must cancel it, or the person who made the *application* to the *Secretary of State* must apply for its cancellation, if he or she is satisfied that the surveillance no longer meets the criteria upon which it was authorised. Where the *senior authorising officer* or person who made the *application* to the *Secretary of State* is no longer available, this duty will fall on the person who has taken over the role of *senior authorising officer* or taken over from the person who made the *application* to the *Secretary of State* or the person who is acting as the *senior authorising officer*.[43]

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

6.34 Following the cancellation of any intrusive surveillance *authorisation*, other than one granted by the *Secretary of State*, the Surveillance Commissioners must be notified of the cancellation.[44]

Authorisations quashed by a Surveillance Commissioner

6.35 In cases where a police, NCA, HMRC or CMA *authorisation* is quashed or cancelled by a Surveillance Commissioner, the *senior authorising officer* must immediately instruct those involved to stop

43 See the Regulation of Investigatory Powers (Cancellation of *Authorisations*) Order 2000; SI No. 2794.

44 This notification shall include the information specified in the Regulation of Investigatory Powers (Notification of *Authorisations* etc.) Order 2000; SI No. 2563.

carrying out the intrusive surveillance. Documentation of the date and time when such an instruction was given should be retained for at least three years (see Chapter 8).

Chapter 7
AUTHORISATION PROCEDURES FOR PROPERTY INTERFERENCE

General basis for lawful activity

7.1 *Authorisations* under section 5 of the 1994 Act or Part III of the 1997 Act should be sought wherever *member*s of the intelligence services, the police, the *services police*, NCA, HMRC or CMA, or persons acting on their behalf, conduct entry on, or interference with, property or with wireless telegraphy that would be otherwise unlawful.

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

7.3 In many cases an operation using covert techniques may involve both directed or intrusive surveillance and property interference. This can be authorised as a combined *authorisation*, although the criteria for *authorisation* of each activity must be considered separately (see above, 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 the 2000 Act). In this case, the necessity and proportionality of the property interference element of the authorisation would need to be considered by the appropriate authorising officer separately to the necessity and proportionality of obtaining private information by means of the directed surveillance.

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

Informed consent

7.5 *Authorisations* under the 1994 Act and 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 Part II of the 2000 Act depending on the operation.

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

Incidental property interference

7.6 The 2000 Act 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* or *warrant* is not capable of being granted or might not reasonably have been expected to have been sought under any existing legislation.[45] 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 1994 Act or 1997 Act is available but might not reasonably have been expected to be sought (perhaps due to the unforeseeable nature or location of the activity).

7.7 Where an *authorisation* for the incidental conduct is not available (for example because the 1994 Act or 1997 Act do 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 27(2) of the 2000 Act. 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.

45 See section 27(2) of the Act.

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

Samples

7.8 The acquisition of samples, such as DNA samples, fingerprints and footwear impressions, where there is no consequent loss of or damage to property does not of itself constitute unlawful property interference. However, wherever it is necessary to conduct otherwise unlawful property interference to access and obtain these samples, an *authorisation* under the 1994 or 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 48(2) of the 2000 Act. The appropriate lawful authority in these cases is likely to be the Data Protection Act.

Example 1: Police wish to take fingerprints from a public telephone to identify a suspected criminal who is known recently to have used the telephone. The act of taking the fingerprints would not involve any unlawful property interference so no authorisation under the 1994 or 1997 Act is required. The subsequent recording and analysis of the information obtained to establish the individual's identity would not amount to surveillance and therefore would not require authorisation under the 2000 Act.

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 1994 or 1997 Act where it would otherwise be unlawful.

Authorisations for property interference by the police, the services police, NCA, HMRC and CMA

7.9 Responsibility for these *authorisations* rests with the *authorising officer* as defined in section 93(5) of the 1997 Act, i.e. the chief constable or equivalent. *Authorisations* require the personal authority of the *authorising officer* (or their designated deputy) except in urgent situations, where it is not reasonably practicable for the *application* to be considered by such person. The person entitled to act in such cases is set out in section 94 of the 1997 Act.

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

- it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime;[46] and
- that the taking of the action is proportionate to what the action seeks to achieve.

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

46 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. Where the *authorising officer* is the Chair of the CMA, the only purpose falling within this definition is the purpose of preventing or detecting an offence under section 188 of the Enterprise Act 2002 (see section 93(2AA) of the 1997 Act.

Collaborative working and regional considerations

7.12 *Authorisations* for the police, the *services police*, NCA, HMRC and CMA may only be given by an *authorising officer* on *application* by a *member* or *officer* of the same force or agency unless, in the case of the police, a relevant collaboration agreement has been made which permits this rule to be varied.

7.13 *Authorisations* for the police may only be given for property interference within the *authorising officer*'s own area of operation unless, in the case of the police, a relevant collaboration agreement has been made which permits this rule to be varied. Unless a relevant collaboration agreement applies, an *authorising officer* may authorise property interference (excluding wireless telegraphy interference) outside the relevant area, solely for the purpose of maintaining (including replacing) or retrieving any device, apparatus or equipment the use of which within the relevant area has been authorised under the 1997 Act or 2000 Act. Unless a relevant collaboration agreement applies, an *authorisation* for maintenance or retrieval outside of the *authorising officer*'s own area of operations can only be given for circumstances that do not require entry onto private land.

7.14 Any person granting or applying for an *authorisation* or *warrant* to enter on or interfere with property or with wireless telegraphy will also need to be aware of particular sensitivities in the local community where the entry or interference is taking place and of similar activities being undertaken by other *public authorities* which could impact on the deployment. In this regard, it is recommended that the *authorising officers* in the *services police*, NCA, HMRC and CMA should consult a senior *officer* within the police force 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 *officer*s maintaining (including replacing) or retrieving equipment in Northern Ireland.

Authorisation procedures

7.15 *Authorisations* will generally be given in writing by the *authorising officer*. However, in urgent cases, they may be given orally by the *authorising officer*. In such cases, a statement that the *authorising officer* has expressly authorised the action(s) should be recorded in writing by the applicant as soon as is reasonably practicable, together with that information detailed below.

7.16 If the *authorising officer* is absent then an *authorisation* can be given in writing or, in urgent cases, orally by the designated deputy as provided for in section 94(4) of the 1997 Act, section 12(A) of the Police Act 1996, section 18 of the Police and Fire Reform (Scotland) Act 2012, section 25 of the City of London Police Act 1839 or section 93(5) of the 1997 Act (for NCA).

7.17 Where, however, in an urgent case, it is not reasonably practicable for the *authorising officer* or designated deputy to consider an *application*, then written *authorisation* may be given by the following:

- in the case of the police, by an assistant chief constable (other than a designated deputy);[47]
- in the case of the Metropolitan Police and City of London Police, by a commander;
- in the case of MOD police or British Transport Police, by a deputy or assistant chief constable;
- in the case of the *services police*, by an assistant Provost Marshal (in the Royal Naval Police) or deputy Provost Marshal (in the Royal Military Police or Royal Air Force Police);
- in the case of NCA a person designated by the Director General;
- in the case of HMRC, by a person designated by the Commissioners of Revenue and Customs;[48]
- in the case of the CMA, by an *officer* of the CMA designated for this purpose.

47 ACPO out-of-hours *officer*s of assistant chief constable rank or above will be entitled to act for this purpose.

48 This will be an *officer* of the rank of assistant chief investigation *officer*.

Information to be provided in applications

7.18 *Applications* to the *authorising officer* for the granting or renewal of an *authorisation* must be made in writing (unless urgent) by a police *officer*, Revenue and Customs *officer,* a *member* of NCA or an *officer* of the CMA 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 which the entry or interference with will affect;
- the nature and extent of the proposed interference;
- the details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why the intrusion is justified;
- details of the offence suspected or committed;
- how the *authorisation* criteria (as set out above) have been met;
- any action which may be necessary to maintain any equipment, including replacing it;
- any action which may be necessary to retrieve any equipment;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and
- whether an *authorisation* was given or refused, by whom and the time and date on which this happened.

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

- the identity or identities of those owning or using the property (where known);
- sufficient information to identify the property which will be affected;
- details of the offence suspected or committed;
- the reasons why the *authorising officer* or designated deputy considered the case so urgent that an oral instead of a written *authorisation* was given; and/or

- the reasons why (if relevant) it was not reasonably practicable for the *application* to be considered by the *authorising officer* or the designated deputy.

Notifications to Surveillance Commissioners

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

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

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

Cases requiring prior approval of a Surveillance Commissioner

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

- any of the property specified in the *authorisation*:
  - is used wholly or mainly as a dwelling or as a bedroom in a hotel; or
  - constitutes office premises;[49] 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

7.24 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).

7.25 In cases requiring prior approval by a Surveillance Commissioner, the duration of an *authorisation* is calculated from the time at which the person who gave the *authorisation* was notified that the Surveillance Commissioner had approved it. This can be done by presenting the *authorising officer* with the approval decision page to note in person or if the *authorising officer* is unavailable, sending the written notice by auditable electronic means. In cases not requiring prior approval, this means from the time the *authorisation* was granted.

7.26 Written *authorisations* given by the persons specified in 7.16 (section 94 of the 1997 Act) and oral *authorisations* given in urgent cases by:

- *authorising officers*; or
- designated deputies

49 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).

will cease at the end of the period of 72 hours beginning with the time when they took effect.

Renewals

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

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

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

Cancellations

7.30 The *senior authorising officer* who granted or last renewed the *authorisation* must cancel it if he or she is satisfied that the *authorisation* no longer meets the criteria upon which it was authorised. Where the *senior authorising officer* is no longer available, this duty will fall on the person who has taken over the role of *senior authorising officer* or the person who is acting as the *senior authorising officer* (see the Regulation of Investigatory Powers (Cancellation of *Authorisations*) Order 2000; SI No. 2794).

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

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

Retrieval of equipment

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

7.34 Where a Surveillance Commissioner quashes or cancels an *authorisation* or renewal, he or she will, if there are reasonable grounds for doing so, order that the *authorisation* remain effective for a specified period, to enable *officer*s to retrieve anything left on the property by virtue of the *authorisation*. He or she can only do so if the *authorisation* or renewal makes provision for this. A decision by the Surveillance Commissioner not to give such an order can be the subject of an appeal to the Chief Surveillance Commissioner.

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

7.35 Once an *authorisation* or renewal expires or is cancelled or quashed, the *authorising officer* must immediately give an instruction to cease all the actions authorised for the entry on or interference with

property or with wireless telegraphy. The time and date when such an instruction was given should be centrally retrievable for at least three years (see Chapter 8).

Authorisations for property interference by the intelligence services

7.36 An *application* for a *warrant* must be made by a *member* of the intelligence services for the taking of action in relation to that agency. In addition, the Security Service may make an *application* for a *warrant* to act on behalf of the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ). SIS and GCHQ may not be granted a *warrant* for action in support of the prevention or detection of serious crime which relates to property in the British Islands.

7.37 The intelligence services should provide the same information as other agencies, as and where appropriate, when making *applications* for the grant or renewal of property *warrant*s.

7.38 Before granting a *warrant*, the *Secretary of State* must:

- think it necessary for the action to be taken for the purpose of assisting the relevant agency in carrying out its functions;
- be satisfied that the taking of the action is proportionate to what the action seeks to achieve;
- take into account in deciding whether an *authorisation* is necessary and proportionate whether the information which it is thought necessary to obtain by the conduct authorised by the *warrant* could reasonably be obtained by other means; and
- be satisfied that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of disclosure of any material obtained by means of the *warrant*, and that material obtained will be subject to those arrangements.

Renewals of intelligence services warrants

7.39 A *warrant* shall, unless renewed, cease to have effect at the end of the period of six months beginning with the day on which it was issued (if the *warrant* was issued under the hand of the *Secretary of State*) or at the end of the period ending with the fifth working day following the day on which it was issued (in any other case).

7.40 If at any time before the day on which a *warrant* would cease to have effect the *Secretary of State* considers it necessary for the *warrant* to continue to have effect for the purpose for which it was issued, he or she may by an instrument under his or her hand renew it for a period of six months beginning with the day it would otherwise cease to have effect.

Cancellations of intelligence services warrants

7.41 The *Secretary of State* shall cancel a *warrant* if he or she is satisfied that the action authorised by it is no longer necessary.

7.42 The person who made the *application* to the *Secretary of State* must apply for its cancellation, if he or she is satisfied that the *warrant* no longer meets the criteria upon which it was authorised. Where the person who made the *application* to the *Secretary of State* is no longer available, this duty will fall on the person who has taken over from the person who made the *application* to the *Secretary of State* (see the Regulation of Investigatory Powers (Cancellation of *Authorisations*) Order 2000; SI No. 2794).

Retrieval of equipment by the intelligence services

7.43 Because of the time it can take to remove equipment from a person's property it may also be necessary to renew a property *warrant* in order to complete the retrieval. *Applications* to the *Secretary of State* for renewal should state why it is being or has been closed down, why it has not been possible to remove the equipment and any timescales for removal, where known.

Chapter 8
KEEPING OF RECORDS

Centrally retrievable records of authorisations

Directed and intrusive surveillance authorisations

8.1 A record of the following information pertaining to all *authorisations* shall be centrally retrievable within each *public authority* for a period of at least three years from the ending of each *authorisation*.[50] This information should be regularly updated whenever an *authorisation* is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request. More guidance for local authorities on the recording of magistrates' decisions is available in Home Office-issued guidance available on the gov.uk website.

- the type of *authorisation*;
- the date the *authorisation* was given;
- name and rank/grade of the *authorising officer*;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- for local authorities, details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- the dates of any reviews;

50 See also paragraph 8.4.

- if the *authorisation* has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the *authorising officer*;
- whether the investigation or operation is likely to result in obtaining *confidential information* as defined in this code of practice;[51]
- whether the *authorisation* was granted by an individual directly involved in the investigation;[52]
- the date the *authorisation* was cancelled.

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

- a copy of the *application* and a copy of the *authorisation* together with any supplementary documentation and notification of the approval given by the *authorising officer*;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the *authorising officer*;
- a record of the result of each review of the *authorisation*;
- a copy of any renewal of an *authorisation*, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction to cease surveillance was given;
- the date and time when any other instruction was given by the *authorising officer*;
- for local authorities a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace (JP).

51 See Chapter 4.

52 See paragraph 5.7.

Property interference authorisations

8.3 The following information relating to all *authorisations* for property interference should be centrally retrievable for at least three years:[53]

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

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

53 See also paragraph 8.4.

Chapter 9
HANDLING OF MATERIAL AND USE OF MATERIAL AS EVIDENCE

Use of material as evidence

9.1 Subject to the provisions in Chapter 4 of this code, material obtained through directed or intrusive surveillance, or entry on, or interference with, property or wireless telegraphy, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984[54] and the Human Rights Act 1998.

9.2 Any decisions by a Surveillance Commissioner in respect of granting prior approval for intrusive surveillance activity or entry on, or interference with, property or with wireless telegraphy, shall not be subject to appeal or be liable to be questioned in any court.[55]

Retention and destruction of material

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

54 And section 76 of the Police & Criminal Evidence (Northern Ireland) Order 1989.

55 See section 91(10) of the 1997 Act.

9.4 Where the product of surveillance or interference with property or wireless telegraphy could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements[56] for a suitable further period, commensurate to any subsequent review.

9.5 There is nothing in the 2000 Act, 1994 Act or 1997 Act which prevents material obtained under directed or intrusive surveillance or property interference *authorisations* from being used to further other investigations.

Law enforcement agencies

9.6 In the cases of the law enforcement agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

The intelligence services, MOD and HM Forces

9.7 The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.

9.8 With regard to the service police forces (the Royal Navy Police, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the Criminal Procedure and Investigations Act 1996 (Code of Practice) (Armed Forces) Order 2008, which requires that the investigator retain all material obtained in a service investigation which may be relevant to the investigation.

56 For example, under the Criminal Procedure and Investigations Act 1996.

Chapter 10
OVERSIGHT BY COMMISSIONERS

10.1 The 1997 and 2000 Acts require the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police (including the service police forces, the Ministry of Defence Police and the British Transport Police), NCA, HMRC and the other *public authorities* listed in Schedule 1 of the 2000 Act and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 and, in Northern Ireland, officials of the Ministry of Defence and HM Forces.

10.2 The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within Part II of the 2000 Act and the 1994 Act by the Security Service, Secret Intelligence Service, GCHQ and the Ministry of Defence and HM Forces (excluding the service police forces, and in Northern Ireland officials of the Ministry of Defence and HM Forces).

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

10.4 References in this code to the performance of review functions by the Chief Surveillance Commissioner and other Commissioners apply also to Inspectors and other *member*s of staff to whom such functions have been delegated.

Chapter 11
COMPLAINTS

11.1 The 2000 Act establishes an independent Tribunal. This Tribunal will be made up of senior *member*s of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

☎ 020 7035 3711

Chapter 12
GLOSSARY

Application	A request made to an *authorising officer* to consider granting (or renewing) an *authorisation* for directed or intrusive surveillance (under the 2000 Act), or interference with property or wireless telegraphy (under the 1994 or 1997 Act). An *application* will be made by a *member* of a relevant *public authority*.
Authorisation	An *application* which has received the approval of an *authorising officer*. Depending on the circumstances, an *authorisation* may comprise a written *application* that has been signed by the *authorising officer*, or an oral *application* that has been verbally approved by the *authorising officer*.
Authorising officer	A person within a *public authority* who is entitled to grant *authorisations* under the 2000 or 1997 Acts or to apply to the *Secretary of State* for such *warrants*. Should be taken to include *senior authorising officers*.
Confidential information	Confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between *Members of*

	Parliament and their constituents, or matters subject to *legal privilege*. See Chapter 4 for a full explanation.
Legal privilege	Matters subject to *legal privilege* are defined in section 98 of the 1997 Act. This includes certain communications between professional legal advisers and their clients or persons representing the client.
Member	An employee of an organisation, or a person seconded to that organisation.
Member of Parliament	Is reference to a Member of both Houses of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly, and Northern Ireland Assembly.
Officer	An *officer* of a police force, HMRC, or the CMA, or a person seconded to one of these agencies as an *officer*.
Private information	Any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. *Private information* includes information about any person, not just the subject(s) of an investigation.
Public authority	Any public organisation, agency or police force (including the military police forces).

Secretary of State	Any *Secretary of State* (in practice this will generally be the Home Secretary).
Senior authorising officer	A person within a *public authority* who is entitled to grant intrusive surveillance *authorisations* under the 2000 Act or to apply to the *Secretary of State* for such *warrants*. See also *Authorising officer*.
Services police	The Royal Naval Police, Royal Military Police or Royal Air Force Police.
Warrant	A type of *authorisation* granted by a *Secretary of State* following an *application* for intrusive surveillance or property interference under the 1994, 1997 or 2000 Acts.

Annex A
Authorisation levels when knowledge of confidential information is likely to be acquired

Relevant public authority	Authorisation level
Police Forces:	
Any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London)	Chief Constable
The Police Service of Scotland	Chief Constable
The Metropolitan police force	Assistant Commissioner
The City of London police force	Commissioner
The Police Service of Northern Ireland	Deputy Chief Constable
The Ministry of Defence Police	Chief Constable
The Royal Navy Police	Provost Marshal
The Royal Military Police	Provost Marshal
The Royal Air Force Police	Provost Marshal
The National Crime Agency	Deputy Director General
The Serious Fraud Office	A Member of the Senior Civil Service or Head of Domain
The Intelligence Services:	
The Security Service	Deputy Director General

Relevant public authority	Authorisation level
The Secret Intelligence Service	A Director of the Secret Intelligence Service
The Government Communications Headquarters	A Director of GCHQ
HM Forces:	
The Royal Navy	Rear Admiral
The Army	Major General
The Royal Air Force	Air-Vice Marshal
The Commissioners for HM Revenue and Customs	Director Investigation, or Regional Heads of Investigation
The Department for Environment, Food and Rural Affairs:	
DEFRA Investigation Services	Head of DEFRA Investigation Services
Marine and Fisheries Agency	Head of DEFRA Prosecution Service
Centre for Environment, Fisheries and Aquaculture Science	Head of DEFRA Prosecution Service
The Department of Health:	
The Medicines and Healthcare Products Regulatory Agency	Chief Executive of the Medicines and Healthcare Products Regulatory Agency

Relevant public authority	Authorisation level
The Home Office	Senior Civil Service pay band 1 with responsibility for criminal investigations in relation to immigration and border security
The Ministry of Justice	Chief Executive Officer of the National Offender Management Service
The Northern Ireland Office: The Northern Ireland Prison Service	Director or Deputy Director Operations in the Northern Ireland Prison Service
The Department of Business, Innovation and Skills	The Director of Legal Services A
The Welsh Assembly Government	Head of Department for Health and Social Services, Head of Department for Health and Social Services Finance, Head of Rural Payments Division, Regional Director or equivalent grade in the Care and Social Services Inspectorate for Wales
Any county council or district council in England, a London borough council, the Common Council of the City of London in its capacity as a local authority, the Council of the Isles of Scilly, and any county council or borough council in Wales	The Head of Paid Service, or (in his/her absence) the person acting as the Head of Paid Service

Relevant public authority	Authorisation level
The Environment Agency	Chief Executive of the Environment Agency
The Prudential Regulation Authority	Chief Executive of the Prudential Regulation Authority
The Competition and Markets Authority	Chair of the Competition and Markets Authority
The Financial Conduct Authority	Chairman of the Financial Conduct Authority
The Food Standards Agency	Head of Group, or Deputy Chief Executive or Chief Executive of the Foods Standards Agency
The Health and Safety Executive	Director of Field Operations, or Director of Hazardous Installations Directorate
NHS bodies in England and Wales: A Special Health Authority established under section 28 of the National Health Service Act 2006 or section 22 of the National Health Service (Wales) Act 2006	Managing Director of the NHS Counter Fraud and Security Management Services Division of the NHS Business Services Authority
The Royal Pharmaceutical Society of Great Britain	Deputy Registrar and Director of Regulation
The Department of Work and Pensions: Jobcentre Plus	Chief Executive of Jobcentre Plus

Relevant public authority	Authorisation level
The Royal Mail Group Ltd, by virtue of being a Universal Service Provider within the meaning of the Postal Services Act 2000	Director of Security

This code of practice provides guidance and rules on authorisations for the carrying out of surveillance (directed surveillance and intrusive surveillance) under Part 2 of the Regulation of Investigatory Powers Act 2000 and for interference with property or with wireless telegraphy under Part 3 of the Police Act 1997. It sets out the various authorisation procedures to be followed for the grant, review, renewal and cancellation of authorisations, as well as special rules for authorisations in respect of confidential and legally privileged information.

The code is aimed primarily at members of public authorities involved in making applications for the grant of authorisations and those persons designated to grant authorisations.

TSO
information & publishing solutions

www.tso.co.uk

ISBN 978-0-11-341373-7

9 780113 413737