NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, ITALICS AND DOUBLE-UNDERLINED

[REDACTION]

NOTE FOR FILE

[REDACTION]

Copied To: ***Deputy Director General, legal adviser, senior officials, lawyer***

[REDACTION]

Date: 15 November 2007

SUBJECT: Visit of the IPT to Thames House – 28 September 2007

Summary

- IPT visit Security Service on 28 September 2007 for general briefing;
- First visit since 2002;
- Specific presentations on data-handling techniques and impact on Service response to IPT complaints;
- **IPT members do not question our assertion that research of 'reference data' in response to a complaint was neither necessary nor proportionate;**
- **A *statement/summary of intended future practice* is attached at Annex C.**

[REDACTION]

Detail

1. After months of struggling to get as many members of the IPT as possible available on the same day, the following attended a briefing at Thames House hosted by ***Deputy Director General***:

Lord Justice Sir John Mummery (President of the Tribunal)

Sheriff Principal John McInnes QC

Peter Scott QC

Sir Richard Gaskill

Robert Seabrook QC

Veronica Selio OBE (Tribunal Registrar)

Sue Cavanagh (Secretary to the Tribunal and Commissioners)

Mr Justice Burton (Vice-President) and Mr William Carmichael (IPT member who is shortly to retire) were unable to attend.

2. The programme for the visit is attached (Annex B). The main objective was to educate the tribunal members in our data-handling techniques including our gathering and storage of bulk data and to seek to obtain their agreement that the searching of this 'reference data' was not necessary or proportionate when responding to an IPT complaint. A description of this discussion [REDACTION] is attached at Annex A. In short, although the IPT seemed to accept our arguments on this issue, we did not push to obtain their explicit agreement to continue to restrict our search for a complainant's details to the data sets that the Service has created.

3. The secondary objective [REDACTION] was to brief them on the growth in and changes to the Service and, in particular, on the scale of the threat that the Service was facing. [REDACTION]

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, ITALICS AND DOUBLE-UNDERLINED

[REDACTION]

ANNEX A

Account of the Data Handling Presentation to the IPT and the following discussion on Conduct and Service response to IPT complaints

1. ***Senior official*** (assisted by [REDACTION]) explained the nature and extent of the Service's data holdings, including the distinction between:

(a) **Service data generated on individuals in the course of Service investigations** – i.e. this includes people in respect of whom we have generated data whether or not they themselves are targets; and

(b) **reference data** – which consist of large datasets (i.e. our bulk data-sets) about the general population, and which help us to (i) identify targets from fragments of intelligence, and (ii) track their activities. ***The relevant teams*** used three practical examples (including an introduction to the ***analytical systems***) to demonstrate the benefit to national security provided by reference data and the steps we take to satisfy the tests of **necessity** and **proportionality**.

2. In discussion following these presentations and over lunch, we (***Deputy Director General, legal adviser, senior officials, lawyer***) told the IPT that the breadth and nature of the reference data we hold is such that [REDACTION] the issue for us was what threshold it was sensible for us to adopt in practice for providing a positive response to a query from the IPT. We suggested that our approach should be as set out in paragraph 3 below.

3. In the event of a complaint:

(a) The Service will search the databases and other records that it has created to record details of investigative targets ***and others***.

(b) If the search produces a "hit", we will confirm to the IPT that we hold a record on the complainant and provide it with an account of why, and of the investigation or other action we have undertaken in relation to the complaint, including any relevant authorisations. [REDACTION] Nor will we check our reference data generally for any mentions of the complainant's name, unless such data was relevant to and/or actively relied on in the course of the investigation.

(c) If the complaint does NOT produce a "hit", we will inform the IPT that we do not hold a record on the complainant, though they may well appear in one of our reference datasets. In such cases, we will not check our reference data generally for any mention of the complainant's name. [REDACTION]

4. We made the point that taking action to check our reference data generally would involve creating an intrusion/interference with privacy which would not otherwise have occurred, and that this did not seem to the Service either sensible or necessary for the purposes of section 65 of RIPA.

5. In the course of the subsequent discussion, we suggested that the approach suggested under paragraph 3(a) and (b) above would adequately meet the IPT's need to be able to judge whether the Service had engaged in any

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, ITALICS AND DOUBLE-UNDERLINED

[REDACTION]

unauthorised conduct in relation to the complainant or otherwise acted improperly towards him, and took account of our need to have a workable system.

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, ITALICS AND DOUBLE-UNDERLINED

[REDACTION]

ANNEX B

Visit of the Investigatory Powers Tribunal
Friday 28 September 2007

Lord Justice Sir John Mummery (President of the Tribunal)
Sheriff Principal John McInnes QC
Peter Scott QC
Sir Richard Gaskill
Robert Seabrook QC
Veronica Selio OBE (Tribunal Registra)
Sue Cavanagh (Secretary to the Tribunal and Commissioners)

DG's Conference Room

10:00	Arrival at Thames House	*senior official* to meet
10:05	Welcome and introduction	*Deputy Director General*
10:15	[REDACTION]	
10:45	[REDACTION]	
11:30	Data handling in National Security work.	*senior officials*
12:30	Lunch (*Deputy Director General, legal adviser, senior officials, lawyer*)	
13:45	[REDACTION]	
14:30	[REDACTION]	
15:15	Wash-up	*Deputy Director General, legal adviser*
15:30	End	

[REDACTION]

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, ITALICS AND DOUBLE-UNDERLINED

[REDACTION]

ANNEX C

statement/summary of intended future practice

[REDACTION] we should make it clear that our usual practice is not generally also to check those records held by the Service which purely consist of reference data-bases, containing information about the population generally (e.g. the Voters' Roll), for any mention of the complainant's name. We would only do this if the data in those records was relevant to or had been relied on in the course of an investigation. If, on the other hand, we were to carry out such a check on the complainant's details, this would involve creating an unnecessary intrusion or interference with privacy which would not otherwise have occurred, and for which there could be no national security justification. We do not believe that it is necessary to do this in order for the Tribunal to be able to satisfy itself that the Service has not engaged in any unauthorised conduct in relation to the complainant or otherwise acted improperly. [REDACTION]

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 *members* 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 *officers* 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.