Home Office

Covert Surveillance and Property Interference

Draft Revised Code of Practice

June 2018

Covert Surveillance and Property Interference

Draft Revised Code of Practice

Presented to Parliament pursuant to section 71(4)
of the Regulation of Investigatory Powers Act 2000

June 2018

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at RIPA@homeoffice.x.gsi.gov.uk

ISBN 978-1-5286-0492-5

CCS0618781142 06/18

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationary Office

Contents

1 Introduction

1.1 This code of practice provides guidance on the use by public authorities of Part II of the Regulation of Investigatory Powers Act ("the 2000 Act") to authorise covert surveillance that is likely to result in the obtaining of private information[1] about a person. The code provides guidance on when an application should be made for an authorisation under the 2000 Act and the procedures that must be followed before activity takes place. The code also provides guidance on the handling of any information obtained by surveillance activity.

1.2 The code also applies to the entry on, or interference with, property or with wireless telegraphy by public authorities. Chapter 7 of this code provides guidance on the issue of warrants under section 5 of the Intelligence Services Act 1994 ("the 1994 Act") or authorisations under Part III of the Police Act 1997 ("the 1997 Act").

1.3 This code is issued pursuant to Section 71 of the 2000 Act, which provides that the Secretary of State shall issue one or more codes of practice in relation to the powers and duties in Part 2 of the 2000 Act, section 5 of the 1994 Act and Part III of the 1997 Act. This code replaces the previous Covert Surveillance and Property Interference code of practice (dated December 2014). This version of the code reflects changes introduced by the Investigatory Powers Act 2016 ("the 2016 Act"), including the introduction of equipment interference warrants under Part 5 of the 2016 Act and the new oversight framework, establishing the Investigatory Powers Commissioner ("the Commissioner")[2]. The previous arrangements, set out in the code of practice issued in December 2014 should be applied, until the relevant provisions of the 2016 Act have been commenced.

1.4 This code of practice is primarily intended for use by the public authorities able to authorise activity under the 2000 Act, the 1994 Act and Part III of the 1997 Act. It will also allow other interested persons to understand the procedures to be followed by those public authorities. This code is publicly available and should be readily accessible by members of any relevant public authority seeking to authorise covert surveillance or entry on, or interference with, property or with wireless telegraphy.

1.5 The 2000 Act provides that all codes of practice issued under the Act are admissible as evidence in criminal and civil proceedings. Any court or tribunal considering such proceedings, the Investigatory Powers Tribunal , or the Investigatory Powers Commissioner responsible for overseeing the relevant powers and functions, may take the provisions of the codes of practice into account. Public authorities may also be required to justify, with regard to this code, the use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

---

[1] See paragraph 3.3 to 3.6 of this code for more detail on private information

[2] Further information on oversight by the Investigatory Powers Commissioner and the Judicial Commissioners is provided at chapter 10 of this code

1.6 Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are included for guidance only. It is not possible for theoretical examples to replicate the level of detail to be found in real cases. Consequently, public authorities 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 the law, including the provisions of this code. The examples should not be taken as confirmation that any particular public authority undertakes the activity described; examples are for illustrative purposes only.

2 Activity by public authorities to which this code applies

Covert surveillance

2.1 Part II of the 2000 Act provides for the authorisation of covert surveillance by public authorities listed at Schedule 1 of the 2000 Act where that surveillance is likely to result in the obtaining of private information about a person.

2.2 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].

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

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

- Directed surveillance is covert surveillance that is not intrusive and 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);

- 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].

2.5 Chapter 3 of this code provides a fuller description of directed and intrusive surveillance, along with definitions of terms, exceptions and examples. Surveillance carried out as part of an equipment interference warrant issued under the 2016 Act does not require a separate authorisation under the 2000 Act (see paragraphs 3.41 to 3.44 below).

[3] See section 48(2) of the 2000 Act

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

[5] See chapter 3 of this code for full definition of residential premises and private vehicles, and note that the 2010 Legal Consultations Order identified a new category of surveillance to be treated as intrusive surveillance (see chapter 9).

Interference with property and wireless telegraphy

2.6 Part 3 of the 1997 Act provides for the authorisation of property interference (entry onto or interference with property or with wireless telegraphy) by law enforcement bodies listed in section 93(5) of the 1997 Act and at 7.1 of this code. Similarly, section 5 of the 1994 Act provides for warrants, issued by the Secretary of State to the intelligence services, authorising entry on or interference with property or with wireless telegraphy. Chapter 7 of this code provides a fuller description of such authorisations and the interaction with equipment interference warrants provided for in the 2016 Act.

Basis for lawful activity

2.7 The Human Rights Act 1998 gave effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, while others are qualified, meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied.

2.8 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. Property interference activity may also engage Article 1 of the First Protocol, the right to peaceful enjoyment of possessions, which could include any property subject to interference by public authorities. 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.

2.9 Part II of the 2000 Act, Part III of the 1997 Act and section 5 of the 1994 Act, provide a statutory framework under which covert surveillance or property interference activity can be authorised and conducted compatibly with the ECHR.

Relevant public authorities

2.10 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 Part I and Part II of Schedule 1 of the 2000 Act.
- Intrusive surveillance applications may only be made by those public authorities whose senior authorising officer is listed in 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 section 93(5) of the 1997 Act and at 7.1 of this code; or (under section 5 of the 1994 Act) by the intelligence services.

Scotland

2.11 Where covert surveillance is authorised, all of which is likely to take place in Scotland, authorisations should be granted under the Regulation of Investigatory Powers (Scotland) Act 2000 ("RIP(S)A 2000")[6], 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.

2.12 Intrusive surveillance authorisations given by the intelligence services where all of the conduct is likely to take place in Scotland can be subject to approval by Scottish Ministers, as outlined in paragraph 6.7 to 6.9 of this code.

2.13 Section 76 of RIPA allows for cross border operations. An authorisation under RIP(S)A 2000 will allow Scottish public authorities to conduct surveillance anywhere in the UK for a period of up to three weeks at a time. This three week period will restart each time the border is crossed, provided it remains within the original validity of the authorisation.

2.14 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 Covert Surveillance and Property Interference Code of Practice, published by the Scottish Government, applies in relation to authorisations granted under RIP(S)A 2000.

International considerations

2.15 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 overseas is to take place, RIPA authorisation can provide a defence under UK law, and the risks of any liability arising under local law should be considered and mitigated where possible.

2.16 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.

2.17 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, UK military bases and detention facilities.

---

[6] Section 46(1)(b)

2.18 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 paragraphs 5.25 to 5.27 (foreign surveillance teams operating in the UK) for detail.

2.19 Under the 1997 Act, property interference authorised to be undertaken by police forces must take place within the "relevant area", which is normally the force area in which they operate. The public authorities able to authorise property interference under the 1997 Act to which this constraint does not apply[7], should apply the considerations set out at 2.16 above to any property interference activity overseas which they are able to undertake in accordance with their statutory functions.

2.20 Section 22A of the Police Act 1996 provides for police forces (including the NCA) to enter into collaboration agreements where the chief officers of two or more police forces consider any police functions, such as covert surveillance, can be discharged more effectively when members of those forces act jointly. Further detail on such collaboration agreements is at para 4.29 to 4.33 of this code.

2.21 For property interference activity carried out overseas by the intelligence services, an authorisation under section 7 of the 1994 Act may be available, provided the Secretary of State is satisfied that:

- The acts are necessary for the proper discharge of a function of the relevant intelligence service;
- Satisfactory arrangements are in force to secure that nothing will be done beyond that which is necessary for the proper discharge of a function, and that the nature and likely consequences will be reasonable having regard for these purposes; and
- Satisfactory arrangements are in force with respect to disclosure of information, in accordance with the 1994 Act.

Activity to which this code does not apply

2.22 This code does not provide guidance for interference with property or wireless telegraphy that is for the purpose of acquiring communications (as defined by section 135 of the 2016 Act), equipment data or other information falling within the definition of 'equipment data', as defined by section 100 of the 2016 Act and covered by the Equipment Interference code of practice.

[7] Public authorities other than police forces i.e. the NCA, HM Revenue and Customs, Home Office Immigration and Competition and Markets Authority (see s93(1B) of the 1997 Act).

2.23 Applicants for a property interference authorisation or warrant will therefore need to consider whether the property with which they intend to interfere falls within the definition of equipment in the 2016 Act, and whether the interference is carried out to obtain communications, equipment data or other information. If the acquisition of communications, equipment data or other information is incidental and not the purpose of the interference, then this activity may be authorised as property interference. Otherwise, the intelligence services should seek authorisation as equipment interference under the 2016 Act where the relevant intelligence service considers that the conduct would otherwise constitute an offence under the Computer Misuse Act 1990 and there is a British Islands connection (see section 13 of the 2016 Act). Law enforcement agencies may obtain an equipment interference warrant under the 2016 Act, or use one of their other statutory powers. See also paragraphs 7.1 – 7.3 of this code.

2.24 Where covert surveillance activities are unlikely to result in the obtaining of any private information about a person, no interference with Article 8 rights occurs and an authorisation under the 2000 Act is therefore not applicable and this code does not apply. It should be assumed that intrusive surveillance will always result in the obtaining of private information.

2.25 Similarly, an authorisation under the 1997 or 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, section 64A of the Police and Criminal Evidence Act 1984[8] (1984 Act) provides a legal basis for the police to, in certain specified circumstances, covertly record images of a suspect for the purposes of identification and obtaining certain evidence.

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

[8] See also the Police & Criminal Evidence (Northern Ireland) Order 1989.

3 Directed and intrusive surveillance overview

This chapter provides further guidance on whether covert surveillance activity is directed surveillance or intrusive surveillance, and whether an authorisation for either activity is available.

Directed surveillance

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

- it is covert, but not intrusive surveillance[9];
- 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.

3.2 Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person. Chapter 5 below provides further information about the authorisation of directed surveillance.

Private information

3.3 The 2000 Act states that private information includes any information relating to a person's private or family life[10]. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family[11] and professional or business relationships. Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

---

[9] Defined at paragraph 3.19 of this code

[10] See section 26(10) of the 2000 Act.

[11] Family should be treated as extending beyond the formal relationships created by marriage or civil partnership.

3.4 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.[12] Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites. See paragraphs 3.10 to 3.17 below for further guidance about the use of the internet as a surveillance tool.

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

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

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

3.6 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[13].

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*

---

[12] Note also that a person in police custody will have certain expectations of privacy.

[13] 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.

these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.

Specific situations requiring directed surveillance authorisations

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

- Section 26(4) of the 2000 Act provides that the use of surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle is not considered to be intrusive surveillance. The use of such devices alone does not necessarily constitute directed surveillance as they do not necessarily provide private information about any individual, but sometimes only supply information about the location of that particular device at any one time. However, the use of that information in a way that would amount to the covert monitoring of the movements of the occupants of the vehicle, or when coupled with other surveillance activity which may obtain private information about the occupants of the vehicle, could interfere with Article 8 rights, so a directed surveillance authorisation may therefore be appropriate. A property interference authorisation may also be appropriate for the covert installation of the device[14].

- Surveillance consisting in 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 by 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[15] authorising the interception.[16]

[14] The use of such devices is also likely to require a warrant for property interference under the 1994 or an authorisation under the 1997 Act (see chapter 7 of this code), or it may fall to be authorised under the equipment interference provisions of the 2016 Act to which a separate code of practice applies.

[15] i.e. under Part 2 or Part 6 Chapter 1 of the 2016 Act

[16] 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 Chapter 1 of Part 2 of the 2016 Act in these circumstances.

Recording of telephone conversations

3.8 Subject to paragraph 3.7 above, the interception of communications sent by public post or by means of public telecommunication system or private telecommunications is governed by Part 2 and Chapter 1 of Part 6 of the 2016 Act. Nothing in this code should be taken as granting dispensation from the requirements of those Parts of the 2016 Act, which are governed by the Interception of Communications Code of Practice.

3.9 The recording or monitoring of one or both ends of a telephone conversation by a surveillance device as part of an authorised directed (or intrusive) surveillance operation will not constitute interception under Part 2 or Chapter 1 of Part 6 of the 2016 Act provided the process by which the product is obtained does not involve any modification of, or interference with, the telecommunication 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 telecommunication 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 mechanical 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 telecommunication system.*

Online covert activity

3.10 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6.

Example 1: *A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

Example 2: *A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*

Example 3: *A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

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

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

Example: *Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.*

Aerial covert surveillance

3.18 Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'), is planned, the same considerations outlined in chapters 3 and 5 of this code should be made to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude. (See also 3.36 to 3.39 of this code with regard to overt surveillance cameras.)

Example: *An unmanned aircraft deployed by a police force to monitor a subject of interest at a public demonstration is likely to require an authorisation for directed surveillance, as it is likely that private information will be obtained and those being observed are unaware it is taking place, regardless of whether the drone is marked as belonging to the police force. Unless sufficient steps have been taken to ensure that participants in the demonstration are aware that aerial surveillance will be taking place, such activity should be regarded as covert.*

Intrusive surveillance

3.19 Intrusive surveillance is covert surveillance that is:

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

3.20 If surveillance activity falls within the definition of intrusive surveillance, this has the effect of reducing the number of public authorities able to carry out such surveillance to a small number of law enforcement agencies and the intelligence services (see paragraph 6.1 below). It will also make authorisations in respect of such surveillance subject to prior approval by either an independent Judicial Commissioner (for law enforcement agencies) or the Secretary of State (for the intelligence services).

3.21 The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained, as it is assumed that intrusive surveillance will always be likely to result in the obtaining of private information. Accordingly, it is not necessary to consider whether or not intrusive surveillance is likely to result in the obtaining of private information.

3.22 In addition, directed surveillance under certain circumstances described within Article 3(2) of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 ("2010 Legal Consultations Order") is to be treated as intrusive surveillance. See paragraph 3.28 and chapter 9 of this code for further information about the 2010 Legal Consultations Order and authorisation of intrusive surveillance.

Residential premises

3.23 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.[17] 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.[18]

3.24 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.

3.25 Examples of residential premises would therefore include:

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

3.26 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);

[17] See section 48(1) of the 2000 Act

[18] See section 48(7) of the 2000 Act

- a prison canteen or police interview room;
- a hotel reception area or dining room;
- the front garden or driveway of premises readily visible to the public;
- residential premises occupied by a public authority for non-residential purposes, for example trading standards 'house of horrors' situations or undercover operational premises.

Private vehicles

3.27 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.[19] This is distinct to vehicles owned or leased by public authorities, further detail on which is provided at paragraph 7.49 to 7.50 of this code.

Places for Legal Consultation

3.28 The 2010 Legal Consultations Order provides that directed surveillance that is carried out on premises ordinarily used for legal consultations, at a time when they are being used for legal consultations, is to be treated as intrusive surveillance for the purposes of Part II of the 2000 Act. Article 3(2) of the Order specifies that the relevant premises for these purposes are:

- 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;
- 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;
- police stations;
- any place in which persons may be detained under Part VI of the Criminal Procedures (Scotland) Act 1985, the Mental Health (Care and Treatment) (Scotland) Act 2003 or the Mental Health Act 2003;
- the place of business of any professional legal adviser; and
- any place used for the sittings and business of any court, tribunal, inquest or inquiry.

3.29 Further information on the 2010 Legal Consultations Order is detailed at paragraphs 9.65 to 9.68 of this code.

[19] See section 48(1) and 48 (7) of the 2000 Act

Further considerations

3.30 Intrusive surveillance (or directed surveillance being treated as intrusive surveillance under the 2010 Legal Consultations 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.[20]

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.*

Activity not falling within the definition of covert surveillance

3.31 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 obtained for such activity. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to the statutory grounds specified in the 2000 Act;
- overt use of CCTV and ANPR systems[21];
- covert surveillance authorised as part of an equipment interference warrant under the 2016 Act;
- certain other specific situations (see paragraph 3.40).

Each situation is detailed and illustrated below.

[20] See section 26(5) of the 2000 Act.

[21] Unless used as part of a specific operation or investigation, likely to obtain private information. See paragraphs 3.36 to 3.39 below.

Immediate response

3.32 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 or monitor social media accounts during a public order incident.*

General observation activities

3.33 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. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation.

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

Example 2: *Police officers monitoring publicly accessible information on social media websites, using a general search term (such as the name of a particular event they are policing), would not normally require a directed surveillance authorisation. However, if they were seeking information relating to a particular individual or group of individuals, for example, by using the search term "group x" (even where the true identity of those individuals is not known) this may require authorisation. This is because use of such a specific search term indicates that the information is being gathered as part of a specific investigation or operation, particularly in circumstances where information is recorded and stored for future use.*

Example 3: *Local authority officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of*

particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again this is part of the general duties of public authorities and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.

***Example 4:** 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 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 5:** 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

3.34 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 is necessary on the grounds specified in the 2000 Act (specified at section 28(3) for directed surveillance and at section 32(3) for intrusive surveillance). 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.

3.35 The 'core functions' referred to by the Investigatory Powers Tribunal[22] are the 'specific public functions', undertaken by a particular public authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc.). These "ordinary functions" are covered by the Data Protection Act 2018 and the Information Commissioner's Employment Practices Code. A public authority may only seek authorisations under the 2000 Act when in performance of its 'core functions'. For example, the disciplining of an employee is not a 'core function', although related criminal investigations may be. As a result, the protection afforded by an authorisation under the 2000 Act may be available in relation to associated criminal investigations, so long as the activity is deemed to be necessary and proportionate.

[22] C v The Police and the Secretary of State for the Home Office - IPT/03/32/H dated 14 November 2006

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.*

Example 2: *A police officer is suspected to be removing classified information from the work environment and sharing it improperly. The police force wishes to investigate the matter by undertaking covert surveillance of the employee. The misconduct under investigation amounts to the criminal offence of misfeasance in a public office, and therefore the proposed investigation relates to the core functions of the police, and the proposed surveillance is likely to result in the obtaining of private information. Consequently, a directed surveillance authorisation should be considered.*

Example 3: *It is alleged that a public official has brought their department into disrepute by making defamatory remarks online, and identifying themselves as a public official. The department wishes to substantiate the allegations separately from any criminal action. Such activity, even if it is likely to result in the obtaining of private information, does not constitute directed surveillance for the purposes of the 2000 Act, as it does not relate to the discharge of the department's core functions.*

Overt surveillance cameras - CCTV and ANPR (Automatic Number Plate Recognition)

3.36 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 ("the 2012 Act") and overseen by the Surveillance Camera Commissioner. Public authorities should also be aware of the relevant Information Commissioner's code ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information").

3.37 The Surveillance Camera code has relevance to overt surveillance camera systems (as defined at s29(6) of the 2012 Act) and which are operated in public places by relevant authorities (defined at s 33(5) of the 2012 Act) in England and Wales. The 2012 Act places a statutory responsibility upon those public authorities defined by the 2012 Act, to have regard to the provisions of the Surveillance Camera code, where surveillance is conducted overtly by means of a surveillance camera system in a public place in England and Wales.

3.38 The Surveillance Camera code sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the Data Protection Act 2018 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.*

3.39 However, where overt CCTV, ANPR or other overt surveillance 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, ANPR or other overt surveillance cameras 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 he remains unaware that there may be any specific interest in him. This targeted, covert use of the overt town centre CCTV system to monitor and/or record that individual's movements should be considered for authorisation as directed surveillance.*

Specific situations where authorisation is not available

3.40 The following specific activities constitute neither directed nor intrusive surveillance:

- the use of a recording device by a covert human intelligence source in respect of whom an appropriate use or conduct authorisation has been granted permitting him or her to record any information obtained in their presence; [23]

- the recording, whether overt or covert, of an interview with a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a member of a public authority. In such circumstances, whether the recording equipment is overt or covert, the member of the public knows that they are being interviewed by a member of a public authority and that information gleaned through the interview has passed into the possession of the public authority in question;

[23] See section 48(3) of the 2000 Act

- 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 available;

- 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;[24]

- 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).[25]

Covert surveillance authorised by an equipment interference warrant

3.41 The obtaining of communications or information, authorised by a targeted equipment interference warrant issued under Part 5 the 2016 Act, includes obtaining those communications or information by surveillance. This could include intrusive surveillance or directed surveillance.

3.42 A separate authorisation for surveillance under Part II of RIPA will not therefore be required, providing the conduct comprising the surveillance is properly authorised by a targeted equipment interference warrant. The interference with privacy and property resulting from the surveillance will be considered as part of the equipment interference warrant.

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

3.44 For example, if a public authority capable of conducting activity under an equipment interference warrant, also wishes to conduct separate surveillance (e.g. by directing an officer to observe the user of a device at the same time as the device itself is being subject to equipment interference), then this will not be considered as part of the conduct authorised by an equipment interference warrant and the additional surveillance activity must be appropriately authorised. In these circumstances a combined warrant may be appropriate (for information on combined warrants, see paragraphs 4.20 to 4.28 below).

[24] See section 26(6) of the 2000 Act

[25] See section 48(3) of the 2000 Act

4 General rules on authorisations

Overview

4.1 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. Section 32 of the 2000 Act provides for lawful authorisation to be given by those listed to members of their organisations to carry out intrusive surveillance. Similarly, an authorisation under section 5 of the 1994 Act or Part III of the 1997 Act will provide lawful authorisation for members of the intelligence services and law enforcement bodies[26] to enter on, or interfere with, property or wireless telegraphy.

4.2 Responsibility for granting authorisations varies depending on the nature of the operation and the public authority involved. The relevant public authorities and authorising officers[27] for authorisations under Part II of the 2000 Act are detailed in the Schedule to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 RIPA Order") for directed surveillance, and section 32 of the 2000 Act for intrusive surveillance respectively. The public authorities capable of conducting interference with property or wireless telegraphy, under an authorisation or warrant, are set out in the 1994 and 1997 Acts.

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

Necessity and proportionality

4.4 The 2000 Act, 1997 Act and 1994 Act all stipulate that the person granting an authorisation or issuing a warrant for directed or intrusive surveillance, or interference with property, must believe that the activities to be authorised are necessary on one or more statutory grounds.[28]

---

[26] Paragraph 7.1 of this code details those law enforcement organisations capable of such authorisations

[27] An authorising officer is a person within a public authority who is entitled to grant authorisations under the 2000 or 1997 Acts. The term should be taken to include senior authorising officers.

[28] 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 of this code for directed surveillance, intrusive surveillance and interference with property respectively.

4.5 If the activities are deemed necessary on one or more of the statutory grounds, the person granting the authorisation or issuing the 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.

4.6 The authorisation or warrant 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 the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

4.7 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
- 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 information sought;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

4.8 It is important that all those involved in undertaking directed or intrusive surveillance activities under the 2000 Act, or interference with property under the 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.*

4.9 The fact that the information that would be obtained under the authorisation or warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that an authorisation or warrant is necessary on the grounds on which the authorisation or warrant may be granted or issued. Public authorities are permitted, for example, to apply for an authorisation against members or officials of a trade union considered to be a legitimate intelligence target where that is necessary for one or more of the statutory purposes and proportionate to what is sought to be achieved.

4.10 When completing an application for a warrant or authorisation, the public authority must ensure that the case for the warrant or authorisation is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation.

Collateral intrusion

4.11 Before authorising applications for directed or intrusive surveillance or property interference, the authorising officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance or property interference activity (collateral intrusion). Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament and another person on constituency business may be involved (see chapter 9).

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

4.13 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 mitigating the intrusion by not recording or retaining any material obtained through such collateral intrusion.*

4.14 In order to give proper consideration to collateral intrusion, an authorising officer or person considering issuing the warrant should be given full information regarding the potential scope of the anticipated surveillance or interference, including the likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the authorising officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. The authorising officer or person considering issuing the warrant should ensure appropriate safeguards for the handling, retention or destruction of such material in accordance with chapter 9 of this code, as well as compliance with data protection requirements.

4.15 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 4.4 to 4.10).

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

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

Example: *If an individual provides the police with passwords and log-in details for their personal social networking accounts in order to provide evidence of threats made against them, this would not normally require a directed surveillance authorisation. If the police then decided to monitor the accounts for the purposes of obtaining further evidence of criminal activity by the author of the threats, they should consider applying for a directed surveillance authorisation in circumstances where private information is likely to be obtained. This is because the police would be acting with the intention to monitor an*

individual who has not consented to and may not be aware of the surveillance. The public authority will also need to consider the extent of the collateral intrusion into the privacy of others who may comment on or post information onto the accounts under surveillance.

Combined authorisations

4.17 A single authorisation may combine:

- any number of authorisations under Part II of the 2000 Act;[29]
- an authorisation under Part II of the 2000 Act[30] and an authorisation under Part III of the 1997 Act;
- a warrant for intrusive surveillance under Part II of the 2000 Act[31] and a warrant under section 5 of the 1994 Act;
- a targeted interception or equipment interference warrant under the 2016 Act and a warrant under section 5 of the 1994 Act or authorisation under Part III of the 1997 Act (for entry on or interference with property or wireless telegraphy).
- A targeted interception or equipment interference warrant under the 2016 Act and an authorisation for directed or intrusive surveillance under the 2000 Act.

4.18 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 Judicial Commissioner, unless the case is urgent.

4.19 The above considerations do not preclude public authorities from obtaining separate authorisations. Where separate authorisations are sought, consideration should be given to whether reference to these in the related warrants or authorisations is appropriate.

[29] see section 43(2) of the 2000 Act

[30] on the application of a member of a police force, NCA, a customs officer, an officer of Home Office Immigration, or an officer of the CMA. See section 33(5) of the 2000 Act

[31] on the application of a member of the intelligence services. See section 42(2) of the 2000 Act

Combinations involving warrants under the Investigatory Powers Act 2016

4.20 Where any warrant or authorisation under the 2000 or 1997 Act or warrant under the 1994 Act is combined with a warrant under the 2016 Act, the authorisation processes in the 2016 Act will apply[32]. In some cases this will necessitate a higher authorisation process than would otherwise be required for individual applications. Where warrants/authorisations are combined, that would otherwise be issued/authorised by different authorities (for example, a property interference authorisation issued by a law enforcement chief and an interception warrant issued by a Secretary of State), the combined warrant will always be issued by the higher authorisation level. Where one of the warrants or authorisations within a combined warrant is cancelled, the whole warrant ceases to have effect. For example, if conduct required for an operation was authorised by a combined property interference and interception warrant and interception was no longer necessary and proportionate, the whole warrant must be cancelled and a new property interference authorisation or warrant should be sought to cover the property interference that remains necessary and proportionate. Such combined warrants may also be applied for on an urgent basis.

4.21 Where warrants of different durations are combined, the shortest duration applies, except for where a combined warrant issued by the Secretary of State on the application of the head of an intelligence service and with the approval of a Judicial Commissioner includes an authorisation for directed surveillance – in this case, the duration of the warrant is six months.

4.22 The requirements that must be met before an authorisation can be granted or warrant can be issued apply to each part of a combined warrant. For example, where a combined warrant includes a property interference authorisation, all the requirements that would have to be met for a property interference authorisation to be issued should be met by the combined warrant.

4.23 The duties imposed by section 2 of the 2016 Act (having regard to privacy) apply to combined warrants as appropriate. The considerations that apply when deciding whether to issue, renew, cancel or modify a warrant under the 2016 Act will apply when such a warrant forms part of a combined warrant. So the property interference or surveillance element of a combined warrant cannot be issued without having regard to privacy in accordance with section 2 of the 2016 Act.

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

[32] Warrants granted under the 1994 Act do not require Judicial Commissioner approval but, when combined with a warrant under the 2016 Act, require Commissioner approval for the 2016 Act element(s)

4.25 Paragraph 20 of Schedule 8 to the 2016 Act provides that various rules regarding warrants apply separately to the relevant part of a combined warrant. The duty of operators to give effect to a warrant applies separately in relation to each part of a combined warrant. So, for example, section 128 (duty of operators to assist with implementation) would apply to the targeted equipment interference part of a combined warrant but only to that part.

4.26 Similarly, safeguards also apply to individual parts of a combined warrant. For example, where a combined targeted equipment interference and intrusive surveillance warrant has been issued, the safeguards that apply to a targeted equipment interference warrant apply to the part of the combined warrant that is a targeted equipment interference warrant.

4.27 When a property interference or surveillance authorisation is combined with an interception warrant, the material derived from property interference or surveillance may in principle be used in legal proceedings if required, whilst the exclusion of matters from legal proceedings continues to apply to material obtained under the interception.[33] However, if material derived from property interference or surveillance authorised by a combined warrant reveals the existence of an interception warrant, the material is excluded from use in legal proceedings according to section 56 of the 2016 Act.

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

Collaborative working

4.29 Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance or property interference is taking place, and of any similar activities being undertaken by other public authorities which could impact on the deployment of surveillance or property interference. 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.

4.30 In cases where one agency or force is acting on behalf of another, the tasking agency should normally obtain or provide the authorisation. For example, where surveillance is carried out by the police on behalf of HMRC, the authorisation would usually be sought by HMRC and granted by the appropriate authorising officer within HMRC, despite the fact that the surveillance activity is being conducted by the police. Where the operational support of other agencies (in this example, the police) is foreseen, this should be specified in the authorisation.

[33] Further detail contained in chapters 11 and 12 of the interception code of practice

4.31 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.

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

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

- HMRC applications for directed or intrusive surveillance and property interference, and CMA applications for intrusive surveillance, must only be made by a member or officer of the same organisation as the authorising officer, regardless of which force or agency is to conduct the activity.

- 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 Officers 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[34].

- Police 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 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.

[34] Following amendment of the Police Act 1996 Act by the Policing and Crime Act 2017, the NCA may also be included in such arrangements.

Reviewing authorisations and warrants

4.34 Regular reviews of all authorisations and warrants 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 and warrants frequently where the surveillance or property interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information[35] is likely to be obtained.

4.35 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. References to the authorising officer in paragraphs 4.36 and 4.37 below should be taken to include the officer responsible for reviewing Secretary of State authorisations.

4.36 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 or warrant should continue or whether the criteria on which he or she based the original decision to grant an authorisation or warrant have changed sufficiently to cause the authorisation or warrant 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 or warrant in the same terms.

4.37 Any proposed or unforeseen changes to the nature or extent of the activity 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 or warrant is to be renewed.

4.38 Where a directed or intrusive surveillance authorisation or warrant provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation or warrant 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 or warrant, providing the scope of the original authorisation or warrant envisaged surveillance of such individuals. Such changes must be highlighted at the next renewal if the authorisation or warrant is to be renewed.

---

[35] 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 9 of this code for further detail.

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".*

4.39 During a review, the reviewing officer may cancel aspects of the authorisation or warrant, for example to cease directed surveillance against one of a number of named subjects or to discontinue the use of a particular tactic.

General best practice

4.40 The following guidelines should be considered as best working practices by all public authorities with regard to all applications for warrants or 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 and the requirements of this code[36];
- the case for the warrant or authorisation should be presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which support or weakens the case for the warrant or authorisation;
- where warrants or authorisations are granted orally under urgency procedures (see chapters 5, 6 and 7 of this code 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 or warrants should not generally be sought for activities already authorised following an application by the same or a different public authority.

[36] As laid out in chapters 5, 6 and 7 of this code

4.41 Furthermore, it is considered good practice that within every relevant public authority, a senior responsible officer[37] 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, section 5 of the 1994 Act and with this code;
- oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Investigatory Powers Commissioner and inspectors who support the Commissioner when they conduct their inspections;
- where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Judicial Commissioner, and
- ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

Local authorities

4.42 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.

4.43 In Scotland this requirement only applies to authorisations for communications data as the use of the other techniques is governed by RIP(S)A 2000. 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.

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

4.44 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 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products. The offences relating to the latter are in article 7A of the 2010 RIPA Order.

- 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 6 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.

4.45 The provisions of the 2012 Order, detailed above, do not apply to Scotland and Northern Ireland.

4.46 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 Investigatory Powers Commissioner. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed.

4.47 Elected members of a local authority should review the authority's use of the 1997 Act and the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 1997 Act and 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.

Covert surveillance of a CHIS

4.48 It may be necessary to deploy covert surveillance against a potential or authorised CHIS, other than those acting in the capacity of an undercover operative, as part of the process of assessing their suitability for recruitment, deployment or in planning how best to make the approach to them. Covert surveillance in such circumstances may or may not be necessary on one of the statutory grounds on which directed surveillance authorisations can be granted, depending on the facts of the case. Whether or not a directed surveillance authorisation is available, any such surveillance must be justifiable under Article 8(2) of the ECHR.

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:

- in the interests of national security;
- for the purpose of preventing or detecting[38] crime or of preventing disorder;
- in the interests of the economic well-being of the UK;
- in the interests of public safety;
- for the purpose of protecting public health[39];
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department[40]; or
- for any other purpose prescribed by an order made by the Secretary of State[41].

5.2 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 relates to the protection of national security and in particular the protection against threats from terrorism, which are the responsibility of the Security Service, 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
- 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.

---

[38] 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.

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

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

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

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

5.4 The authorising officer must also believe that the surveillance is proportionate to what it seeks to achieve (see paragraphs 4.4 to 4.10 above).

Relevant public authorities

5.5 The public authorities entitled to authorise directed surveillance 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 2010 RIPA Order.

Information to be provided in applications

5.6 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 which statutory ground(s) (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 or privileged information[42] that is likely to be obtained as a consequence of the surveillance;
- where the purpose, or one of the purposes, of the authorisation is to obtain information subject to legal privilege[43], an assessment of why there are exceptional and compelling circumstances that make this necessary;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve; and
- the level of authorisation required (or recommended where that is different) for the surveillance.

[42] See paragraphs 9.23 to 9.57 of chapter 9 of this code

[43] See paragraphs 9.51 to 9.53 of chapter 9 of this code

Authorisation procedures

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

5.8 The 2010 RIPA Order designates the authorising officer for each public authority and the officers able to authorise in urgent cases, where applicable. 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. Annex A to this code provides the enhanced authorisation levels for directed or intrusive surveillance by public authorities when knowledge of confidential or privileged information is likely to be acquired.

5.9 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 of this code) should highlight this and the Commissioner or inspector should be invited to view it during his or her next inspection.

Urgent cases

5.10 The authorising officer should generally give authorisations in writing. However, in urgent cases, oral authorisations may be given by the authorising officer. In an urgent oral case, a statement that the authorising officer has expressly authorised the conduct should be recorded in writing by the applicant as soon as is reasonably practicable, together with the information detailed at paragraph 5.13 below.

5.11 In an urgent case, where it is not reasonably practicable having regard to the urgency of the case for the authorising officer to consider the application, an authorisation may be granted in writing by a person entitled to act only in urgent cases under the 2010 RIPA Order.

5.12 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 if an authorisation has been neglected or the urgency is of an administrative nature of the authorising officer or applicant's own making.

5.13 In urgent cases, the information outlined at paragraph 5.6 above 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 paragraph 3.1 of this code;
- the reasons why the authorising officer considered the case so urgent that an oral instead of a written authorisation was given; and,
- where the officer entitled to act in urgent cases has given written authorisation, 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

5.14 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 (or six months for intelligence services' authorisations) beginning with the day when the authorisation granted had taken effect[44]. Even in instances where it is anticipated that an authorisation will only be required for a period of time less than three months, authorisation should still be granted for the statutory three month period, subject to review at an interval reflecting expected duration, and the authorisation cancelled when it is no longer necessary.

5.15 Urgent oral authorisations or written authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after seventy-two hours, beginning with the time when the authorisation granted had taken effect[45].

Renewals

5.16 Section 43 of the 2000 Act provides that authorisations for directed surveillance may be renewed. When considering whether to renew such an authorisation, the authorising officer should give consideration to the same criteria as he would were he considering a new application.

5.17 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 and proportionate, section 44 of the 2000 Act provides that 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.

5.18 If, at any time before an authorisation for directed surveillance granted by an authorising officer in any other public authority 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 seventy-two hours. The renewal will take effect at the time at which the authorisation would have ceased to have effect but for the renewal.

---

[44] Section 43(3)(c)

[45] Section 43(3)(a)

5.19 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.

5.20 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;
- whether any privileged material or confidential information was obtained as a result of activity undertaken under the authorisation, to which the safeguards in chapter 9 of this code should apply;
- the results of regular reviews of the investigation or operation.

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

Cancellations

5.22 The authorising officer must cancel the authorisation at any time if they consider that the directed surveillance no longer meets the criteria upon which it was authorised. Where the original authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer (see the 2010 RIPA Order).

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

5.24 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s) as soon as reasonably practicable. The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained (see chapter 8 below). There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation. However it is good practice 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

5.25 The provisions of section 76A of the 2000 Act[46] provide for foreign surveillance teams to operate in the UK, subject to the following procedures and conditions.

5.26 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 2000), 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).

5.27 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.

[46] Inserted by the Crime (International Co-Operation) Act 2003

6 Authorisation procedures for intrusive surveillance

Authorisation criteria

6.1 An authorisation for intrusive surveillance may be granted by the Secretary of State[47] for applications by the intelligence services, the Ministry of Defence, HM Forces, or any other public authority designated for this purpose under section 41 of the 2000 Act[48], or by a senior authorising officer[49] or designated deputy[50] of the police, National Crime Agency (NCA), HM Revenue and Customs (HMRC), Competition and Markets Authority (CMA), Independent Office for Police Conduct (IOPC) or the Home Office (for departments exercising functions relating to immigration matters and officers designated as customs officials), as listed in section 32(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 or equipment interference. This can be authorised as a combined authorisation, although the criteria for authorisation of each activity must be considered separately (see paragraphs 4.19 to 4.27 above on combined authorisations).

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

i. that the authorisation is necessary in the circumstances of the particular case on the grounds that it is:

- in the interests of national security[51];

[47] Or the Scottish Ministers, provided for under section 63 of the Scotland Act 1998

[48] Only two public authorities have been designated by Order for this purpose: The Regulation of Investigatory Powers (Designation of Public Authorities for the Purposes of Intrusive Surveillance) Order 2001 designated the Ministry of Justice, enabling intrusive surveillance to be carried out in prisons; and the Regulation of Investigatory Powers (Intrusive Surveillance) Order 2003, which designated the Northern Ireland Office for the Northern Ireland Prison Service.

[49] 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.

[50] See section 34(6) of the 2000 Act

[51] 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[52];
- 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

ii. 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.

Information to be provided in all applications

6.5 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 which statutory ground(s) (e.g. for the purpose of preventing or detecting serious crime) listed in section 32(3) and 32(3A)[53] of the 2000 Act;
- the nature of the surveillance;
- the residential premises or private vehicle in relation to which the surveillance will take place, where known;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any confidential or privileged information that is likely to be obtained as a consequence of the surveillance;

[52] 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 twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

[53] For the CMA, for the purpose of preventing or detecting an offence under section 188 of the Enterprise Act 2002 (cartel offence).

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

- the reasons why the surveillance is considered proportionate to what it seeks to achieve.

Authorisation procedures for law enforcement agencies - senior authorising officers and designated deputies

6.6 The senior authorising officers for these bodies are listed in section 32(6) of the 2000 Act. If the senior authorising officer is absent so it is not reasonably practicable for them to consider an application for an authorisation, section 34(2) of the 2000 Act provides that an authorisation can be given by the designated deputy (if there is one). Designated deputies are specified at section 34(6) of the 2000 Act.

Authorisation Procedures for Secretary of State or Scottish Ministers Authorisations

6.7 Intrusive surveillance by any of the intelligence services, the Ministry of Defence, HM Forces or any other public authority designated for this purpose under section 41 of the 2000 Act requires the approval of a Secretary of State, unless these bodies are acting on behalf of another public authority that has obtained an authorisation.

6.8 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.

6.9 Section 42 of the 2000 Act requires that intelligence services authorisations granted by the Secretary of State must be made by issue of a warrant. Such warrants will generally be given in writing by the Secretary of State or member of the Scottish Executive for those issued by the Scottish Ministers. In urgent cases, section 44 of the 2000 Act provides that a warrant may be signed (but not renewed) by a senior official[54], with the express authorisation of the Secretary of State.

Urgent law enforcement cases

6.10 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.

[54] For Scotland, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service and is designated by the Scottish Ministers as a person under whose hand a warrant may be issued in such a case (in this section referred to as "a designated official")

6.11 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.[55]

6.12 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 or applicant's own making.

6.13 In urgent cases, the information in paragraph 6.5 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.

Notifications to a Judicial Commissioner

6.14 Where a person grants, renews or cancels a law enforcement agency authorisation for intrusive surveillance, he or she must, as soon as is reasonably practicable, give notice in writing to the Commissioner, in accordance with whatever arrangements have been made by the Investigatory Powers Commissioner.[56]

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 Judicial 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.

[55] Note that NPCC out-of-hours officers of assistant chief constable rank or above will be entitled to act for this purpose.

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

Judicial Commissioner approval

6.16 Except in urgent cases, a law enforcement agency authorisation granted for intrusive surveillance will not take effect until it has been approved by a Judicial Commissioner and written notice of the Judicial Commissioner's decision has been given to the person who granted the authorisation. This means that the approval will not take effect until the notice has been received in the office of the person who granted the authorisation within the relevant force or organisation.

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

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

Duration of law enforcement intrusive surveillance authorisations

6.19 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).

6.20 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 seventy-two hours beginning with the time when they took effect.

Duration of intelligence service warrants

6.21 A warrant issued to an intelligence service by the Secretary of State or Scottish Ministers will cease to have effect at the end of a period of six months beginning with the day on which it was issued. So a warrant 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 Warrants expressly authorised by a Secretary of State or Scottish Ministers, but signed by a designated 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.

Renewal of law enforcement authorisations

6.23 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. 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.

6.24 As with the initial authorisation, where an authorisation has been renewed by the senior authorising officer or their designated deputy, approval must be sought from a Judicial Commissioner, unless it is a case to which the urgency procedure applies. The renewal will not take effect until the notice of the Judicial Commissioner's approval has been received in the office of the person who granted the authorisation within the relevant force or organisation (but not before the day on which the authorisation would have otherwise ceased to have effect).

6.25 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.

Renewals of Secretary of State warrants

6.26 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.

6.27 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.

6.28 An application for renewal should not be made until shortly before the authorisation period is drawing to an end.

Information to be provided for all renewals of intrusive surveillance authorisations and warrants

6.29 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 6.5;
- the reasons why it is necessary to continue with the intrusive surveillance;

- the details of any confidential or privileged information[57] that is likely to be obtained as a consequence of the surveillance;

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

- the content and value to the investigation or operation of the product so far obtained by the surveillance;

- the results of any reviews of the investigation or operation (see below).

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

Cancellations

6.31 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 may cancel an authorisation at any time, but must apply for its cancellation, if they consider 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.[58]

6.32 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 as soon as reasonably practicable. The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained (see chapter 8 below). 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.

6.33 Following the cancellation of any intrusive surveillance authorisation, other than one granted by the Secretary of State, the Commissioner must be notified of the cancellation.[59]

---

[57] See paras 9.23 to 9.57 of chapter 9 below

[58] See the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794.

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

Authorisations quashed by a Judicial Commissioner

6.34 In cases where a police, NCA, HMRC, IOPC, CMA or Home Office authorisation is quashed or cancelled by a Judicial Commissioner, the senior authorising officer must immediately instruct those involved to stop carrying out the intrusive surveillance. Documentation of the date and time when such an instruction was given should be retained for at least three years (see chapter 8 of this code).

Jurisdictional considerations

6.35 A police or NCA authorisation cannot be granted unless the application is made by a member of the same force or agency, unless a relevant collaboration agreement has been made (see from paragraph 4.29 above, on collaborative working). An authorisation on behalf of another applicable agency cannot be granted unless the application is made by an officer of that agency.

6.36 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 from paragraph 4.29 above).

7 Authorisation procedures for property interference

General basis for lawful activity

7.1 Warrants under section 5 of the 1994 Act or authorisations under Part III of the 1997 Act should be sought wherever members of the intelligence services, the police, the services police[60], National Crime Agency (NCA), HM Revenue and Customs (HMRC), Competition and Markets Authority (CMA), Independent Office for Police Conduct (IOPC), Police Investigations and Review Commissioner, or Home Office (for departments exercising functions relating to immigration matters, and officers designated as customs officials) or persons acting on their behalf, conduct entry on, or interference with, property or with wireless telegraphy that would be otherwise unlawful.[61]

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. However, as noted at paragraph 2.22 above, these property interference powers cannot be used where the proposed interference is for the purpose of acquiring communications, equipment data or other information. In those circumstances:

- Intelligence services are required to apply for an equipment interference warrant under Part 5 of the 2016 Act where the conduct would otherwise constitute an offence under the Computer Misuse Act 1990 and there is a British Islands connection (see section 13 of the 2016 Act).

- The law enforcement agencies are unable to authorise the activity under the Police Act 1997 where the conduct would otherwise constitute an offence under the Computer Misuse Act 1990 (see section 14 of the 2016 Act), but may apply for an equipment interference warrant under Part 5 of the 2016 Act, or use other statutory powers to conduct the activity.

  Example 1: *An agency is seeking to disable a CCTV camera as part of an investigation/operation. The process by which they propose to disable a particular CCTV camera would result in it obtaining a stored copy of footage from the CCTV system. In such circumstances, although the agency is interfering with equipment (the CCTV system) and acquiring communications and/or private information (the footage), the purpose of the interference is to disable the CCTV camera. The acquisition of the CCTV footage is intended, in so far as it is a constituent part of the interference required to disable the CCTV camera, but is entirely incidental. Accordingly, this activity can continue to be authorised as property interference under the 1994 Act or 1997 Act (as applicable).*

[60] The Royal Navy Police, Royal Military Police or Royal Air Force Police

[61] Organisations other than the intelligence services hereafter referred to as the law enforcement agencies in this chapter

Example 2: *An intelligence service is seeking to covertly monitor the movements of a target who has been captured on a CCTV system in the British Islands. In such circumstances, the intelligence service interferes with the CCTV system for the purpose of acquiring a copy of the footage; the purpose of the interference with the equipment is to acquire communications and/or private information and an equipment interference warrant would be required.*

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

Combined warrants and authorisations

7.4 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 or section 5 of the 1994 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.*

7.5 There may be circumstances where both a property interference and equipment interference warrant or authorisation may be required (see paragraphs 4.20 to 4.28 above on combined warrants).

Circumstances where an authorisation or warrant is not required

7.6 A property interference authorisation or warrant 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 an authorisation or warrant 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 or warrant for property interference should be obtained.

Information to be provided in law enforcement applications

7.7 Applications to the authorising officer for the granting or renewal of an authorisation must be made in writing (unless urgent) by a law enforcement agency detailed at paragraph 7.1 above, 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 any information or private information which may be collected as a result of the proposed interference and confirmation that an equipment interference warrant is not applicable given the purpose/nature of the operation investigation;
- details of the offence suspected or committed;
- details of any confidential or privileged information that is likely to be obtained as a consequence of the surveillance[62];
- how the authorisation criteria (as set out below) 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; and
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results.

Authorisation procedures for law enforcement agencies

7.8 Authorisations will be given in writing, and responsibility for these authorisations rests with the authorising officer as defined in section 93(5) of the 1997 Act, i.e. the chief constable or equivalent. Authorisations require the personal authorisation 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.

7.9 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:

[62] See paragraphs 9.23 to 9.64 of chapter 9 of this code.

- it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime[63]; and

- that the taking of the action is proportionate to what the action seeks to achieve.

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

Authorisation procedures for the intelligence services

7.11 An application for a warrant must be made by a member of the intelligence services for the taking of action in relation to that intelligence service. 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.

7.12 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 warrants, as outlined at paragraph 7.7 above.

7.13 Before granting a warrant, the Secretary of State must:

- think it is necessary for the action to be taken for the purpose of assisting the relevant intelligence service 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.

7.14 The Secretary of State or the Scottish Ministers may expressly authorise property interference warrants in urgent cases under section 6(1)(b) or (c) of the 1994 Act. Further detail on urgent cases is provided below.

---

[63] 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).

Urgent cases

7.15 The authorising officer should generally give authorisations in writing. However, in urgent cases, oral authorisations may be given by the authorising officer. In an urgent oral case, a statement that the 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.

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);
- 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;
- in the case of the CMA, by an officer of the CMA designated for this purpose.

7.18 The Secretary of State, or Scottish Ministers where applicable, may authorise a property interference warrant in urgent cases under section 6(1)(b) or (c) of the 1994 Act. The warrant should be endorsed by a senior official with a statement to that effect.

7.19 A case is not normally to be regarded as urgent unless the time that would lapse 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 or applicant's own making.

7.20 In urgent cases, the information at paragraph 7.9 may be supplied orally by those public authorities listed at 7.17 above. 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.

Notification to a Judicial Commissioner

7.21 Where a person gives, renews or cancels an authorisation in respect of entry on or interference with property or with wireless telegraphy under the 1997 Act, he or she must, as soon as is reasonably practicable, give notice of it in writing to a Judicial Commissioner, where relevant, in accordance with arrangements made by the Commissioner. In urgent cases which would otherwise have required the approval of a Judicial Commissioner, the notification must specify the grounds on which the case is believed to be one of urgency.

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

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

Judicial Commissioner approval

7.24 In certain cases, an authorisation under the 1997 Act for entry on or interference with property will not take effect until a Judicial Commissioner has approved it and the notice of approval has been received in the office of the person who granted the authorisation within the relevant force or organisation (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[64]; or

- the action authorised is likely to result in any person incidentally acquiring knowledge of:

  - matters subject to legal privilege;

  - confidential personal information; or

  - confidential journalistic material.

Duration of law enforcement authorisations

7.25 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).

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

7.27 Written authorisations given by the persons specified in 7.17 (section 94 of the 1997 Act) and oral authorisations given in urgent cases by:

a) authorising officers or

b) designated deputies

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

[64] 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).

Renewal of law enforcement authorisations

7.28 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. When considering whether to renew an authorisation, the authorising officer must consider whether authorisation remains both necessary and proportionate, with particular regard to whether the length of the operation means continued interference remains proportionate. Authorisations may be renewed more than once, if necessary, and details of the renewal should be centrally recorded (see chapter 8 below). An application for renewal should not be made until shortly before the authorisation period is drawing to an end.

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

7.30 If, at the time of renewal, criteria exist which would cause an authorisation to require prior approval by a Judicial Commissioner, then the approval of a Judicial Commissioner must be sought before the renewal can take effect. The fact that the initial authorisation required the approval of a Judicial 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).

Duration and renewal of intelligence services warrants

7.31 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).

7.32 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.

Ceasing activity and cancellation of law enforcement authorisations

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

7.34 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 as soon as is reasonably practicable. The time and date when such an instruction was given should be centrally retrievable for at least three years (see chapter 8).

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

7.36 Following the cancellation of the authorisation, the Commissioner 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.

7.37 The Commissioner has 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, the Commissioner may order the destruction of records, in whole or in part, other than any that are required for pending criminal or civil proceedings.

Ceasing activity and cancellation of intelligence services warrants

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

7.39 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.

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

Retrieval of equipment

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

7.42 In such circumstances, it may also be necessary to renew an authorisation or warrant in order to complete the retrieval. Applications to the Secretary of State or authorising officer and notifications to the Commissioner 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.

7.43 Where a Judicial Commissioner quashes or cancels a law enforcement 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 officers 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 Judicial Commissioner not to give such an order can be the subject of an appeal to the Investigatory Powers Commissioner.

7.44 In some cases, a property interference authorisation or warrant may be sought in order to carry out interference that is required due to the cessation of activity authorised under another power. For example, where activity authorised by an equipment interference warrant under the 2016 Act has been completed (no further communications, equipment data or other information is intended to be obtained) and the warrant has been cancelled, but it is determined that further interference with property is required as a consequence of that operation. However, this will not be required if the necessary interference with property is already authorised. For example, if an equipment interference warrant authorises the installation, use and removal of property in order to interfere with equipment, no additional authorisation will be required to carry out consequential interference with property.

Informed consent

7.45 Warrants under the 1994 Act and authorisations under the 1997 Act are not necessary where the public authority is acting with the informed consent of a person able to give permission in respect of the relevant property and actions. However, consideration should still be given to the need to obtain a directed or intrusive surveillance authorisation under 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 available. 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

7.46 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.[65] 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).

[65] See section 27(2) of the Act

7.47 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.

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

7.48 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 available. 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.*

Vehicles or property owned or leased by public authorities

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

record, observe, or listen to other occupants, an authorisation for directed surveillance is required.

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

Collaborative working and regional considerations

7.51 Authorisations for the law enforcement agencies 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 or NCA, a relevant collaboration agreement has been made which permits this rule to be varied.

7.52 Authorisations for the police may only be given for property interference taking place within the authorising officer's own area of operation unless 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.

7.53 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 relevant force or agency 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 officers maintaining (including replacing) or retrieving equipment in Northern Ireland.

8 Record keeping and error reporting

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[66]. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available to the Investigatory Powers Commissioner and inspectors who support the work of the Commissioner 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/warrant;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation (if applicable);
- 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;
- 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 authorised activity is likely to result in obtaining confidential or privileged information as defined in this code of practice[67];
- whether the authorisation was granted by an individual directly involved in the investigation;[68]
- the date the authorisation was cancelled;

---

[66] See also paragraph 8.5

[67] See chapter 9

[68] See paragraph 5.9

- where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner;
- a record of whether, following a refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner;
- where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given.

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).

Property interference authorisations

8.3 The following information relating to all authorisations for property interference should be centrally retrievable for at least three years[69]:

- 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 Judicial Commissioner, if applicable;
- the time and date when the a Judicial Commissioner notified their 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;

[69] See also paragraph 8.5

- the date of every renewal;
- the time and date when any instruction was given by the authorising officer to cease the interference with property or with wireless telegraphy;
- where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner;
- a record of whether, following a refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner;
- where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given.

Collaboration agreements

8.4 Where an authorisation is given under the terms of a Police Act 1996 collaboration agreement, that agreement should explicitly state on which force(s) or agency's central record the authorisation should be recorded. This is likely to be either the force or agency providing the authorising officer, or the designated lead force or agency. The fact that the authorisation was given under these terms should be recorded on the central record.

Retention of records

8.5 Records must be available for inspection by the Investigatory Powers Commissioner and retained to allow the Investigatory Powers Tribunal ('IPT'), established under Part IV of the 2000 Act, to carry out its functions (see chapter 11 below for more information on the IPT). The IPT 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.

Errors

8.6 This section provides information regarding errors. Proper application of the surveillance provisions provided for in Part II of the 2000 Act and the property interference provision provided for in the 1994 and 1997 Acts, should reduce the scope for making errors. Public authorities will be expected to have thorough procedures in place to comply with these provisions, including for example the careful preparation and checking of warrants and authorisations, reducing the scope for making errors.

8.7 Wherever possible, any technical systems should incorporate functionality to minimise errors. A person holding a senior position within each public authority must undertake a regular review of errors and a written record must be made of each review.

8.8 An error must be reported if it is a "relevant error". Under section 231(9) of the 2016 Act, a relevant error for the purpose of activity covered by this code is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act or the property interference provisions of the 1994 and 1997 Acts. Examples of relevant errors occurring would include circumstances where:

- Surveillance or property interference activity has taken place without lawful authorisation.

- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of this Code.

8.9 Errors can have very significant consequences on an affected individual's rights and, in accordance with section 235(6) of the 2016 Act, all relevant errors made by public authorities must be reported to the Investigatory Powers Commissioner by the public authority that is aware of the error.

8.10 When a relevant error has occurred, the public authority that made the error must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner) after it has been established by appropriate internal governance processes that a relevant error has occurred. Such internal governance processes are subject to review by the Investigatory Powers Commissioner. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

8.11 From the point at which the public authority identifies that a relevant error may have occurred, they must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the public authority must also inform the Commissioner of when it was initially identified that an error may have taken place.

8.12 A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days (or as agreed with the Commissioner) of establishing the fact of the error, the reasons this is the case. The report should include information on the cause of the error; the amount of surveillance or property interference conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

8.13 The Investigatory Powers Commissioner may issue guidance as necessary, including guidance on the format of error reports. Public authorities must have regard to any guidance on errors issued by the Investigatory Powers Commissioners.

8.14 In addition to the above, errors may arise where a warrant or authorisation has been obtained as a result of the public authority having been provided with information which later proved to be incorrect due to an error on the part of the person providing the information, but on which the public authority relied in good faith. Whilst these actions do not constitute a relevant error on the part of the authority which acted on

the information, such occurrences should be brought to the attention of the Investigatory Powers Commissioner. Where reporting such circumstances to the Investigatory Powers Commissioner, the processes outlined at paragraph 8.10 apply as they apply to the reporting of a relevant error.

Serious Errors

8.15 Section 231 of the 2016 Act states that the Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

8.16 In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned;
- The extent to which disclosing the error would be contrary to the public interest or prejudicial to:
    - national security;
    - the prevention or detection of serious crime;
    - the economic well-being of the United Kingdom; or
    - the continued discharge of the functions of any of the intelligence services.

8.17 Before making his or her decision, the Commissioner must ask the public authority which has made the error to make submissions on the matters concerned. Public authorities must take all such steps as notified to them by the Investigatory Powers Commissioner to help identify the subject of a serious error.

8.18 When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

9 Safeguards (including privileged or confidential information)

9.1 This chapter provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through directed or intrusive surveillance under the 2000 Act, or property interference under the 1994 or 1997 Act. This material may include private information as defined in section 26(10) of the 2000 Act. It also details the procedures and safeguards to be applied where authorisations or warrants may result in the acquisition of material subject to legal privilege, or other confidential material including journalistic material and the constituency business of Members of Parliament.

9.2 Where this chapter refers to material obtained through property interference, it should be noted that section 13 of the 2016 Act provides the circumstances in which interference by an intelligence service with equipment for the purpose of obtaining communications, private information or equipment data should be authorised as equipment interference under the 2016 Act, rather than under a property interference warrant under the 1994 Act. Section 14 of the 2016 Act provides the circumstances in which interference by a law enforcement agency with equipment for the purpose of obtaining communications, private information or equipment data may not be authorised under a property interference authorisation under the 1997 Act and may be authorised as equipment interference under the 2016 Act (see paragraph 7.2 for more information). Material obtained under an equipment interference warrant is subject to the safeguards set out in the equipment interference code of practice. Paragraphs 9.58 to 9.64 of this chapter set out the limited circumstances in which property interference warrants or authorisations may result in the acquisition of confidential or privileged material and the separate safeguards applicable to such warrants or authorisations.

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

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

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

- is, or is likely to become, necessary for any of the statutory purposes set out in the 2000, 1997 or 1994 Act in relation to covert surveillance or property interference;
- is necessary for facilitating the carrying out of the functions of public authorities under those Acts;
- is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

9.6 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 where it becomes relevant and in accordance with the safeguards in this chapter.

Use of material as evidence

9.7 Subject to the provisions in this chapter of the 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 Criminal Procedure and Investigations Act 1996, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984[70] and the Human Rights Act 1998.

9.8 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the Criminal Procedure and Investigations Act 1996 and these considerations will apply to any material acquired through covert surveillance or property interference that is used in evidence. When information obtained under a covert surveillance or property interference warrant or authorisation is used evidentially, the public authority should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

9.9 Where the product of surveillance or property interference could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In the case 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, which requires that the investigator retain all material obtained in an investigation which may be relevant to the investigation.

[70] and section 76 of the Police & Criminal Evidence (Northern Ireland) Order 1989

9.10 With regard to the service police forces, 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.

Reviewing warrants and authorisations

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

9.12 In each case, unless specified by the authorising officer, Secretary of State or Judicial Commissioner, the frequency of reviews should be determined by the public authority that made the application. This should be as frequently as is considered necessary and proportionate.

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

Handling material

9.14 Paragraphs 9.16 to 9.22 below provide guidance as to the safeguards which govern the dissemination, copying, storage and destruction of private information obtained through covert surveillance or property interference. Each public authority must ensure that there are internal arrangements in force[71] for securing that the requirements of these safeguards are satisfied in relation to private information obtained by these means. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018 and any relevant internal arrangements produced by individual authorities relating to the handling and storage of material.

9.15 Where the intelligence services are obtaining large amounts of data, for example as a result of use of automated surveillance tools, they should also consider whether this material would fall under the provisions on bulk personal datasets in Part 7 of the 2016 Act, and should be subject to the requirements of that Act and the related code of practice.

[71] For the Intelligence Services, these internal arrangements will be approved by the Secretary of State.

Dissemination of information

9.16 Material acquired through covert surveillance or property interference will need to be disseminated both within and between public authorities, as well as to consumers of intelligence (which includes oversight bodies and the Secretary of State, for example), where necessary in order for action to be taken on it. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary for the authorised purpose(s) set out in 9.5 above. This obligation applies equally to disclosure to additional persons within a public authority and to disclosure outside the authority. In the same way, only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

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

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

Copying

9.19 Material obtained through covert surveillance or property interference may only be copied to the extent necessary for the authorised purposes set out at 9.5 above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance or property interference, and any record which refers to the covert surveillance or property interference and the identities of the persons to whom the material relates.

Storage

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

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

- physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems;

- an appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

9.22 Information obtained through covert surveillance or property interference, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out in 9.5 above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible[72].

Confidential or privileged material

9.23 Particular consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source, where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business.[73] Separate guidance on each of these categories of information is set out below.

9.24 Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material may be authorised only by authorising officers entitled to grant authorisations in respect of confidential or privileged information. Annex A to this code lists the authorising officer for each public authority permitted to authorise such surveillance, in circumstances where privileged or confidential information may be acquired. The authorisation levels are set at a more senior level than that required for other surveillance activity, reflecting the sensitive nature of such information. Authorisations for directed surveillance falling within the 2010 Legal Consultations Order must comply with the enhanced authorisation regime set out in that order (see paragraph 9.25 below).

9.25 Intrusive surveillance (including surveillance which is to be treated as intrusive by virtue of the 2010 Legal Consultations Order) likely or intended to result in the acquisition of confidential or privileged material may only be authorised by authorising officers entitled to grant intrusive surveillance (see paragraphs 6.6 and 6.7 above). Such surveillance is also subject to prior approval by a Judicial Commissioner (unless the Secretary of State is the relevant authorising officer or the case is urgent).

---

[72] For example, by taking reasonable steps to make the data unavailable or inaccessible to authorised persons. No further steps are required, such as physical destruction of hardware.

[73] A Member of Parliament is reference to a Member of both Houses of the UK Parliament, the European Parliament, the Scottish Parliament, the National Assembly for Wales, and the Northern Ireland Assembly.

9.26 Property interference under the 1997 Act likely to result in the acquisition of matters subject to legal privilege, confidential personal information or confidential journalistic material may only be authorised by authorising officers entitled to grant property interference authorisations. Such authorisations (unless urgent) are subject to prior approval by a Judicial Commissioner. Such interference is subject to the restriction in section 14 of the 2016 Act, which limits the circumstances in which such activity can be authorised under the 1997 Act (see paragraph 9.2 above).

9.27 Property interference under the 1994 Act likely to result in the acquisition of matters subject to legal privilege, confidential personal information or confidential journalistic material is authorised by the Secretary of State (see paragraphs 9.63 to 9.64 below). Such interference is subject to section 13 of the 2016 Act, which requires activity to be authorised by an equipment interference warrant in certain circumstances, rather than a warrant under the 1994 Act (see para 9.2 above).

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

Confidential personal information and confidential constituent information

9.29 Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or any legal obligation of confidentiality. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

9.30 For the purpose of this code, spiritual counselling is defined as conversations between an individual and a minister of religion acting in his or her official capacity, and where the individual being counselled is seeking, or the minister is imparting, forgiveness, absolution or the resolution of conscience with the authority of the divine being(s) of their faith.

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

9.32 Where the intention is to acquire confidential personal information, or communications of a Member of Parliament, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered by the authorising officer in accordance with the safeguards in this chapter. If the information is exchanged with the intention of furthering a criminal purpose, for example if purported spiritual counselling involves incitement to murder or to acts of terrorism, then the information will not be considered confidential for the purposes of this code. If the acquisition of confidential personal or constituent information is likely but not intended, any possible mitigation steps should be considered by the authorising officer and, if none is available, consideration should be given to whether special handling arrangements are required within the relevant public authority.

9.33 Material which has been identified as confidential personal or confidential constituent information should be retained only where it is necessary and proportionate to do so in accordance with the authorised purpose as set out in 9.5 above or where otherwise required by law. It should be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there should be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised purpose.

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

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

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

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

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

9.38 Confidential journalistic material, as defined by section 100 of the 1997 Act, 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.

9.39 Section 100(2) of the 1997 Act provides that a person holds material in confidence if they hold the material subject to an express or implied undertaking to hold it in confidence, or they hold the material subject to a restriction on disclosure or an obligation of secrecy contained in an enactment. Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist nor the source (for example, a news editor who has been sent some notes by a journalist).

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

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

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

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

9.44 Where material is created or acquired with the intention of furthering a criminal purpose, the material is not to be regarded as having been created or acquired for the purpose of journalism. For example, if a terrorist organisation is creating videos for the promotion or glorification of terrorism according to the UK legal standard, the material cannot be regarded as journalistic material for the purposes of this code and will not attract the safeguards set out in this code. Once material has been broadcast, no confidentiality can attach to the material so it is not confidential journalistic material.

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

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

Items subject to legal privilege – Introduction

9.47 Section 98 of the 1997 Act describes those matters that are subject to legal privilege in England and Wales. In Scotland, the law relating to legal privilege rests on common law principles. In general, communications between professional legal advisers and their clients will be subject to legal privilege unless they are intended for the purposes of furthering a criminal act. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to. These definitions should be used to determine how to classify material obtained through surveillance authorised under the 2000 Act, including through surveillance which is treated as intrusive surveillance as a result of the 2010 Legal Consultations Order (discussed at paragraph 3.22).

9.48 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). Privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by a member of the legal profession, such as advocates, barristers, solicitors or chartered legal executives.

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

9.50 The acquisition of material subject to legal privilege is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR as well as engaging Article 8. The acquisition of material subject to legal privilege (whether deliberate or otherwise) is therefore subject to additional safeguards. Acquisition of such material through property interference is addressed in paragraphs 9.58 to 9.62 below. In relation to covert surveillance, the safeguards provide for three different circumstances where legally privileged items will or may be obtained, as set out in paragraphs 9.51 to 9.57 below. They are:

i) where privileged material is intentionally sought;

ii) where privileged material is likely to be obtained; and

iii) where the purpose or one of the purposes is to obtain items that, if they were not generated or held with the intention of furthering a criminal purpose, would be subject to privilege.

Covert surveillance intended to result in the acquisition of knowledge of matters subject to legal privilege

9.51 Where the intention is for surveillance to acquire knowledge of matters subject to legal privilege (including surveillance which is treated as intrusive surveillance as a result of the 2010 Legal Consultations Order discussed above at paragraph 3.28), the warrant or authorisation application must contain a statement that the purpose, or one of the purposes, of the authorisation is to obtain legally privileged material. Such an authorisation or warrant should only be granted or approved if the authorising officer, Secretary of State or Judicial Commissioner, as appropriate, is satisfied that there are exceptional and compelling circumstances that make the authorisation necessary. Circumstances cannot be exceptional and compelling unless certain conditions are met. Exceptional and compelling circumstances will arise only in a very restricted range of cases, where there is a threat to life or limb or in the interests of national security. The exceptional and compelling test can only be met when the public interest in obtaining the information sought outweighs the public interest in maintaining the confidentiality of legally privileged material, and when there are no other reasonable means of obtaining the required information. The authorised surveillance must be reasonably regarded as likely to yield the intelligence necessary to counter the threat.

Example: *A public authority may need to deliberately monitor legally privileged communications where the legal consultation might yield intelligence that could prevent harm to a potential victim or victims, in addition to the privileged material. For example, if they have intelligence to suggest that an individual is about to conduct a terrorist attack and the consultation may reveal information that could assist in averting the attack (e.g. by revealing details about the location and movements of the individual) then they might want to monitor the legally privileged communications.*

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

9.53 The authorising officer, Secretary of State or Judicial Commissioner will take into account both the public interest in preserving the confidentiality of those particular matters and the broader public interest in maintaining the confidentiality of matters subject to legal privilege more generally. The authorising officer, Secretary of State and Judicial Commissioner must consider that there are exceptional and compelling circumstances that make it necessary to issue the authorisation, and must be satisfied that there are appropriate arrangements in place for the handling, retention, use and destruction of privileged material, and the Secretary of State or Judicial Commissioner must approve the issuing authority's decision. In such circumstances, the authorising officer, Secretary of State and Judicial Commissioner will be able to impose additional requirements such as regular reporting arrangements, so as to keep the authorisation under review more effectively.

Covert surveillance likely to result in the acquisition of knowledge of matters subject to legal privilege

9.54 If the covert surveillance (including surveillance which is treated as intrusive surveillance as a result of the 2010 Legal Consultations Order discussed above at paragraph 3.28) 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 be clear that the acquisition of such matters is likely and should include, in addition to the reasons why the surveillance is considered necessary, an assessment of how likely it is that information which is subject to legal privilege will be obtained. The public authority should also confirm that any inadvertently obtained material that is subject to legal privilege will be treated in accordance with the safeguards set out in this chapter, and that reasonable and appropriate steps will be taken to minimise access to the material that is subject to legal privilege.

Covert surveillance intended to result in the acquisition of knowledge of matters that would be subject to legal privilege if they were not created or held with the intention of furthering a criminal purpose

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

9.56 The requirement to ensure the case for an authorisation is presented in the application in a fair and balanced way, including information which supports or

weakens the case for the warrant or authorisation (as set out in paragraph 4.40) applies in these circumstances as it does elsewhere. For example, information which may undermine the assessment that material is likely to be created or held to further a criminal purpose must also be included in the application to ensure the authorising officer, Secretary of State and Judicial Commissioner can make an informed assessment about the nature of the material.

9.57 The authorisation can only be issued where the authorising officer, Secretary of State or Judicial Commissioner considers that the matters are likely to be created or held with the intention of furthering a criminal purpose. Paragraphs 9.55 to 9.57 apply equally to surveillance which is treated as intrusive surveillance as a result of the 2010 Legal Consultations Order (as discussed above).

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

9.58 As set out in paragraph 9.2 above, section 14 of the 2016 Act restricts the circumstances in which a property interference authorisation under the 1997 Act can be sought. As a result, where the purpose of any interference with property is to obtain communications, private information or equipment data, it will often be authorised under an equipment interference warrant (subject to the safeguards set out in the equipment interference code of practice). Most material subject to legal privilege is likely to fall within the scope of this restriction, so a property interference authorisation under the 1997 Act is unlikely to be available where the purpose (or one of the purposes) is to obtain such material.

9.59 In some cases, it is possible that the purpose of the interference is not to obtain communications, private information or equipment data, but that such material may none the less be acquired incidentally as a result of the interference. In such circumstances, an equipment interference warrant will be unavailable and consideration should be given as to whether any applications for authorisation under the 1997 Act is likely to result in the acquisition of knowledge of matters subject to legal privilege, where the acquisition of knowledge of those matters is incidental to the property interference, and the additional safeguards referred to at paragraph 9.61 below should be applied.

9.60 There may also be cases where the purpose of the interference is to acquire matters subject to legal privilege, but where the activity would not be defined as equipment interference under the 2016 Act, and the safeguards referred to at paragraph 9.61 below should be applied.

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

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

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

9.62 Where the property interference is intended to result in the acquisition of knowledge of matters that would be subject to legal privilege if they were not generated with the intention of furthering a criminal purpose, or held by a person who is not entitled to hold them, the application must include a statement to that effect and the reasons for believing it to be the case.

Property interference under the 1994 Act that may result in the acquisition of knowledge of matters subject to legal privilege

9.63 As set out in paragraph 9.2 above, section 13 of the 2016 Act restricts the circumstances in which a property interference warrant under the 1994 Act can be sought. As a result, where the purpose of any interference with property is to obtain communications, private information or equipment data, it will often be authorised under an equipment interference warrant (and subject to the safeguards set out in the equipment interference code of practice). Most material subject to legal privilege is likely to fall within the scope of this restriction, so a property interference warrant under the 1994 Act is unlikely to be used in many circumstances (as specified in the 2016 Act) where the purpose or one of the purposes is to obtain such material.

9.64 In some cases, it is possible that the purpose of the interference is not to obtain communications, private information or equipment data, but that such material may none the less be acquired incidentally as a result of the interference. There may also be cases where the purpose of the interference is to acquire matters subject to legal privilege, but where the activity would not be defined as equipment interference under the 2016 Act. In such circumstances, an equipment interference warrant will be unavailable, and consideration should be given to whether any application for authorisation under the 1994 Act may result in the acquisition of knowledge of matters subject to legal privilege, and the additional safeguards set out at paragraphs 9.51 to 9.55 above should be applied as if references to surveillance included references to property interference.

Covert surveillance of legal consultations

9.65 The 2010 Legal Consultations 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. As a result, such authorisations are available to a limited range of public authorities and subject to an enhanced authorisation regime including approval by a Judicial Commissioner or the Secretary of State.

9.66 The 2010 Legal Consultations Order defines 'legal consultation' for these purposes as:

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

- 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.

9.67 The definition of 'legal consultation' in the 2010 Legal Consultations 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 and therefore not protected by legal privilege. Covert surveillance of all legal consultations covered by the 2010 Legal Consultations Order (whether protected by legal privilege or not) is to be treated as intrusive surveillance. The locations specified in the Order are outlined at paragraph 3.28 of this code.

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

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

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

9.69 If an authorisation is to be granted by the Secretary of State, the provisions in chapter 6 of this code relating to such authorisations will apply.

Lawyers' material

9.70 Where a lawyer, acting in this professional capacity, is the subject of covert surveillance or property interference, it is possible that a substantial proportion of any material which will or could be acquired will be subject to legal privilege. Therefore, in any case where the subject of covert surveillance or property interference is known to be a lawyer acting in that professional capacity, the application should be made on the basis that it is likely or intended to acquire items subject to legal privilege and the provisions in paragraphs 9.51 to 9.53 will apply, as relevant.

9.71 In relation to covert surveillance, in addition to considering the applicability of the 2010 Legal Consultations Order, the public authority will need to consider which of the three circumstances that apply when items subject to legal privilege will or may be obtained is relevant, and what processes should therefore be followed. In other words, they will need to consider whether items subject to legal privilege are likely to be obtained; whether items subject to legal privilege are intentionally sought; or whether the purpose or one of the purposes is to obtain material that, if it was not created or held with the intention of furthering a criminal purpose, would be subject to privilege. This paragraph does not prevent an application being made on the grounds that the lawyer is under investigation for serious criminal offences, in which case, the application must be made on the basis that it is likely to acquire items subject to legal privilege and the additional considerations set out at paragraph 9.54 will apply.

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

Handling, retention, and deletion of legally privileged material

9.73 In addition to the general safeguards governing the handling and retention of material as provided for in paragraphs 9.16 to 9.22 of this code, authorised persons who analyse material obtained by covert surveillance or property interference should be alert to any communications or items which may be subject to legal privilege. Paragraphs 9.74 to 9.75 below set out the additional arrangements that apply to legally privileged items where the intention is to retain them for a purpose other than their destruction.

9.74 A legal adviser to the public authority must be consulted when it is believed that material which attracts privilege is retained other than for the purpose of destruction. The legal adviser is responsible for determining that material is privileged rather than an officer who is involved in an investigation. In cases where there is doubt as to whether material is privileged or not, the Investigatory Powers Commissioner may be informed, who will be able to give a view. Where it is discovered that privileged material has been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain it for one or more of the authorised purposes (see paragraph 9.5). If not, the material should not be retained, other than for the purpose of its destruction or in accordance with other statutory requirements.

9.75 Material which has been identified as legally privileged (and is being retained for purposes other than its destruction) should be clearly marked as subject to legal privilege and the Investigatory Powers Commissioner must be notified of the retention of the items as soon as reasonably practicable. Paragraphs 9.76 to 9.78 below provide more detail on reporting privileged items to the Commissioner. Such material should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes. Privileged items must be securely destroyed when their retention is no longer needed for those purposes. If such material is retained, there must be adequate information management systems in place to ensure that continued retention, for purposes other than their destruction, remains necessary and proportionate for the authorised statutory purposes.

Reporting to the Commissioner

9.76 In those cases where items identified by a legal adviser to the public authority as being legally privileged have been acquired, this should be reported to the Commissioner as soon as reasonably practicable.

9.77 The Commissioner must order the destruction of the item or impose conditions on its use or retention unless the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. Even if retention is necessary and the public interest in its retention outweighs the public interest in the confidentiality of items subject to legal privilege, the Commissioner may still impose conditions as he considers necessary to protect the public interest in the confidentiality of items subject to privilege.

9.78 It may be the case in some circumstances that privileged items can be retained when their retention does not outweigh the public interest in the confidentiality of items subject to privilege. This includes, for example, where it is not possible to separate privileged items from those that are not privileged and of intelligence value and where the retention is necessary and proportionate for one of more of the authorised purposes or in accordance with statutory requirements. In these circumstances, the Commissioner must impose conditions on the use or retention of the item.

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

Dissemination

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

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

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

10 Oversight

10.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ("the Commissioner"), whose remit includes providing comprehensive oversight of the use of the powers to which this code applies, and adherence to the practices and processes described in it. The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work. The Commissioner will also be advised by the 'Technology Advisory Panel'.

10.2 The Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The Commissioner may undertake these inspections, as far as they relate to the Commissioner's statutory functions, entirely on his or her own initiative. Section 236 of the 2016 Act provides for the Intelligence and Security Committee of Parliament to refer a matter to the Commissioner with a view to carrying out an investigation, inspection or audit.

10.3 The Commissioner will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the Commissioner must not act in a way which is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK (section 229(6) of the 2016 Act). A Commissioner must in particular not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, nor unduly impede the operational effectiveness of an intelligence service, a police force, a government department, or HM Forces (See section 229(7) of the 2016 Act).

10.4 All relevant persons using investigatory powers must provide all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner. Here, a relevant person includes, amongst others, any person who holds, or has held, an office, rank or position within a public authority (see section 235(7) of the 2016 Act).

10.5 Anyone, including anyone working for a public authority, who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner. In particular, any person who exercises the powers described in this code must, in accordance with the procedure set out in chapter 8 of this code, report to the Commissioner any relevant error of which they are aware. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority.

10.6 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to a person who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the person affected. Further information on errors can be found in chapter 8 of this code. The public authority that has made the error will be able to make representations to the Commissioner before the Commissioner decides if it is in the public interest for the person to be informed. Section 231(6) of the 2016 Act states that the Commissioner must also inform the affected person of their right to apply to the Investigatory Powers Tribunal (see chapter 11 of this code for more information on how this can be done).

10.7 The Commissioner must report annually on the findings of their audits, inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the public interest. Only the Prime Minister will be able to make redactions to the Commissioner's report.

10.8 The Commissioner may also report, at any time, on any of their investigations and findings as they see fit. Public authorities may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce whatever guidance they deem appropriate for public authorities on how to apply and use investigatory powers.

10.9 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: www.ipco.org.uk

10.10 Oversight for public authorities in Northern Ireland whose powers have been conferred by Order of the Northern Ireland Assembly is a devolved matter.

11 Complaints

11.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against public authority use of investigatory powers, including those covered by this code, and is the only appropriate tribunal for human rights claims against the intelligence services. Any complaints about the use of powers as described in this code should be directed to the IPT.

11.2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint or claim from a person, the IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination. A 'person' for these purposes includes an organisation, an association, or combination of persons (see section 81(1) of RIPA), as well as an individual.

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

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

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

12 ANNEX A

Enhanced authorisation levels

Applicable to directed and intrusive surveillance authorisations when knowledge of privileged or 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
Police Scotland	Chief Constable
Metropolitan Police	Assistant Commissioner
City of London Police	Commissioner
Police Service of Northern Ireland	Deputy Chief Constable
Ministry of Defence Police	Chief Constable
Royal Navy Police	Provost Marshal
Royal Military Police	Provost Marshal
Royal Air Force Police	Provost Marshal
British Transport Police	Chief Constable
Independent Police Complaints Commission (IPCC)	Chairman of the IPCC, or Deputy Chairman of the IPCC
National Crime Agency	Deputy Director General
Serious Fraud Office	Designated members of the Senior Civil Service
The Intelligence Services:	
Security Service	Deputy Director General
Secret Intelligence Service	A Director of the Secret Intelligence Service
Government Communications Headquarters (GCHQ)	A Director of GCHQ
HM Forces:	
Royal Navy	Rear Admiral
Army	Major General
Royal Air Force	Air-Vice Marshal
HM Revenue and Customs	Director Investigations, or

	Regional Heads of Investigations
Department for Environment, Food and Rural Affairs (DEFRA):	
DEFRA Investigation Services	Head of DEFRA Investigation Services
Centre for Environment, Fisheries and Aquaculture Science	Head of DEFRA Prosecution Service
Marine Management Organisation	MMO Director (Senior Civil Service pay band 1 equivalent)
Department for Health:	
Medicines and Healthcare Products Regulatory Agency	Chief Executive of the Medicines and Healthcare Products Regulatory Agency
Home Office	Senior Civil Service pay band 1 with responsibility for criminal investigations in relation to immigration and border security
Ministry of Justice	Chief Executive of Her Majesty's Prison and Probation Service
Department of Justice Northern Ireland:	
Northern Ireland Prison Service	Director of Reducing Reoffending
Department for Business, Energy and Industrial Strategy:	
The Insolvency Service	Chief Operating Officer
Welsh Government	Director General Health and Social Services Group/Chief Executive NHS Wales Director of Finance Department of Health and Social Services Head of Rural Payments Division Deputy Director, Marine and Fisheries Division'. Head of Department or equivalent grade in the Care Inspectorate of Wales
Any county council or district council in England and Wales, 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	The Head of Paid Service, or (in their absence) the person acting as the Head of Paid Service

Scilly, and any county council or borough council in Wales	
Environment Agency	Chief Executive of the Environment Agency
The Prudential Regulation Authority	Chief Executive of the Prudential Regulation Authority
Competition and Markets Authority	Chair of the Competition and Markets Authority
Financial Conduct Authority	Chairman of the Financial Conduct Authority
Food Standards Agency	Head of Group, or Deputy Chief Executive of the Food Standards Authority
Health and Safety Executive	Director of Regulation
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 Division of the NHS Business Services Authority
General Pharmaceutical Council	Chief Executive and Registrar
Department for Work and Pensions:	
Counter Fraud and Compliance Directorate (CFCD)	CFCD Director
Royal Mail Group Ltd (by virtue of being a Universal Service Provider within the meaning of the Postal Services Act 2000)	Director of Security

CCS0618781142
978-1-5286-0492-5