Home Office

Equipment Interference

Code of Practice

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

January 2016

Home Office

Equipment Interference

Code of Practice

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

January 2016

LONDON: TSO

tso
part of Williams Lea

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

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0333 202 5070
Fax orders: 0333 202 5080
E-mail: customer.services@tso.co.uk
Textphone: 0333 202 5077

TSO@Blackwell and other Accredited Agents

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

ISBN 9780113413942

First published 2016

Printed in the United Kingdom for The Stationery Office.
P002783637 C0.4 02/16 53693 19585

Contents

1. INTRODUCTION

Definitions

In this code:

- "1989 Act" means the Security Service Act 1989;
- "1994 Act" means the Intelligence Services Act 1994;
- "1998 Act" means the Human Rights Act 1998;
- "2000 Act" means the Regulation of Investigatory Powers Act 2000;
- terms in italics (at first use) are defined in the Glossary at the end of this code.

Background

1.1. This code of practice provides guidance on the use by the *Intelligence Services* of section 5 of the Intelligence Services Act 1994 to authorise *equipment interference* to which the code applies. It provides guidance on the procedures that should be followed before equipment interference can take place under that provision, and on the processing, retention, destruction and disclosure of any information obtained by means of the interference.

1.2. 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 section 5 of the 1994 Act. To the extent that the guidance provided by this code with respect to equipment interference under section 5 of the 1994 Act overlaps with the guidance provided by the Covert Surveillance and Property Interference Revised Code of Practice issued in 2014, this code takes precedence. The Intelligence Services should continue to comply with the 2014 Code in all other respects.

1.3. The heads of the Intelligence Services are also under a duty to ensure that arrangements are in force to secure: (i) that no information is obtained by the Intelligence Services except so far as necessary for the proper discharge of their functions;[1] and (ii) that no information is disclosed except so far as is necessary for those functions, for the purpose of any criminal proceedings, and, in the case of the Secret Intelligence Service ("SIS") and the Security Service, for the other purposes specified.[2] The arrangements must include provision with respect to the disclosure of information obtained by virtue of sections 5 and 7, and any information so obtained must be subject to the arrangements.[3]

1.4. There is no power for the Secretary of State to issue codes of practice in relation to the powers and duties in section 7 of the 1994 Act. However, SIS and the Government Communications Headquarters ("GCHQ") should as a matter of policy (and without prejudice as to whether section 6 of the 1998 Act applies) comply with the provisions of this code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of the 1994 Act in relation to equipment located outside the British Islands.[4]

1.5. This code is publicly available and should be readily accessible by members of any of the Intelligence Services seeking to use the 1994 Act to authorise equipment interference to which this code applies.

---

1 See paragraph 1.9.

2 See section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act.

3 See sections 5(2)(c) and 7(3)(c) of the 1994 Act.

4 Applications for authorisations under section 7 may only be made by SIS and GCHQ.

Equipment interference to which this code applies

1.6. This code applies to (i) any interference[5] (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf or in their support, with equipment[6] producing electromagnetic, acoustic and other emissions, and (ii) information derived from any such interference, which is to be authorised under section 5 of the 1994 Act, in order to do any or all of the following:

(a) obtain information from the equipment in pursuit of intelligence requirements;
(b) obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;
(c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);
(d) enable and facilitate surveillance activity by means of the equipment.

"Information" may include communications content, and communications data as defined in section 21 of the 2000 Act.

1.7. The section 5 warrant process should be complied with in order to properly and effectively deal with any risk of civil or criminal liability arising from the interferences with equipment specified at sub-paragraphs (a) to (d) of paragraph 1.6 above. A section 5 warrant provides the Intelligence Services with specific legal authorisation removing criminal and civil liability arising from any such interferences. For the purposes of this code, any activity by the Intelligence Services or persons acting on their behalf or in their support falling within paragraph 1.6 which is (or is to be) authorised under section 5 of the 1994 Act will be referred to as equipment interference.

5 "Interference" for these purposes excludes any interference which takes place with the consent of a person having the right to control the operation or the use of the equipment.

6 "Equipment" may include, but is not limited to, computers, servers, routers, laptops, mobile phones and other devices.

Effect of the code

1.8. The 2000 Act provides that all codes of practice in force under section 71 of the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under the 2000 Act, or to one of the Commissioners carrying out any of their functions under the 2000 Act, it must be taken into account. The Intelligence Services may also be required to justify, with regard to this code, the use of section 5 warrants in general or the failure to apply for or use such warrants where appropriate.

Basis for lawful equipment interference activity

1.9. Equipment interference is conducted in accordance with the statutory functions of each Intelligence Service:

- In the case of the Security Service, the 1989 Act provides that the Service's functions are the protection of national security, the safeguarding of the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands and the provision of support to the police and other law enforcement authorities in the prevention and detection of serious crime;
- For SIS, the 1994 Act provides that its functions are to obtain and provide information relating to the actions or intentions of persons outside the British Islands and to perform other tasks relating to the actions or intentions of such persons in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom, or in the interests of the economic well-being of the United Kingdom or in support of the prevention or detection of serious crime;
- In the case of GCHQ, the 1994 Act provides, as relevant, that its functions are to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material in the interests of national security, with particular reference to the

defence and foreign policies of Her Majesty's Government in the United Kingdom, or in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands, or in support of the prevention or detection of serious crime.

1.10. The Human Rights Act 1998 gives 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, which means that it is permissible for public authorities to interfere with those rights if certain conditions are satisfied.

Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when the Intelligence Services seek to obtain personal information about a person by means of equipment interference. Such conduct may also engage Article 1 of the First Protocol (right to peaceful enjoyment of possessions).[7]

1.11. By section 6(1) of the 1998 Act, it is unlawful for a *public authority* to act in a way which is incompatible with a Convention right. Each of the Intelligence Services is a public authority for this purpose. When undertaking any activity that interferes with ECHR rights, the Intelligence Services must therefore (among other things) act proportionately. Section 5 of the 1994 Act provides a statutory framework under which equipment interference can be authorised and conducted compatibly with ECHR rights.

1.12. So far as any information obtained by means of an equipment interference warrant is concerned, the heads of each of the Intelligence Services must also ensure that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of the disclosure of that information, and that any information obtained under the warrant

7 For example, hardware or software.

will be subject to those arrangements. Compliance with these arrangements will ensure that the Intelligence Services remain within the law and properly discharge their functions.

Application of section 5 of the 1994 Act

1.13. The 1994 Act applies to each of the Intelligence Services in a slightly different way:

- SIS and GCHQ may not be issued with a section 5 warrant for action in support of the prevention or detection of serious crime which relates to equipment in the British Islands;[8]
- The Security Service may only be issued with a section 5 warrant for action in support of the prevention or detection of serious crime which relates to equipment in the British Islands if certain conditions are satisfied.[9]

1.14. The procedures for authorising equipment interference under section 5 (and any associated interferences) are explained further in chapter 4.

8 See section 5(3) of the 1994 Act.

9 See section 5(3B) of the 1994 Act.

2. GENERAL RULES ON WARRANTS

Overview

2.1. A warrant under section 5 of the 1994 Act will, providing the statutory tests are met, remove criminal and civil liability arising from equipment interference operations.

2.2. Responsibility for issuing warrants under section 5 rests with the Secretary of State. Applications for warrants may be made by any of the Intelligence Services.

2.3. In any case where an equipment interference operation also enables or facilitates separate covert surveillance likely to result in the obtaining of private information about a person, a directed or intrusive surveillance authorisation may be required under Part 2 of the 2000 Act (see the Covert Surveillance and Property Interference Code of Practice).

Necessity and proportionality

2.4. The 1994 Act provides that the Secretary of State issuing the warrant must believe that the activities to be authorised are necessary for one or more statutory purposes.[10]

2.5. If the activities are deemed necessary for any of the purposes specified, the Secretary of State must also believe that they are proportionate to what is sought to be achieved by carrying them out.

2.6. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The 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 there is a potential threat to national security (for example) may not alone render the

10 These statutory purposes are specified in section 5 of the 1994 Act. They are detailed in Chapter 4.

most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

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

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

2.8. It is important that all those involved in undertaking equipment interference operations under the 1994 Act are fully aware of the extent and limits of the action that may be taken under the warrant in question.

Collateral intrusion

2.9. Any application for a section 5 warrant should also take into account the risk of obtaining private information about persons who are not subjects of the equipment interference activity (collateral intrusion).

2.10. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the equipment 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.

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

2.12. Where it is proposed to conduct equipment interference activity specifically against individuals who are not intelligence targets in their own right, interference with the equipment of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such equipment interference activity should be carefully considered against the necessity and proportionality criteria as described above.

Reviewing warrants

2.13. Regular reviews of all warrants should be undertaken to assess the need for the equipment interference activity to continue. The results of a review should be retained for at least three years (see Chapter 5). Particular attention should be given to the need to review warrants frequently where the equipment interference involves a high level of intrusion into private life or significant collateral intrusion, or *confidential information* is likely to be obtained.

2.14. In each case, unless specified by the Secretary of State, the frequency of reviews should be determined by the member of the Intelligence Services who made the application. This should be as frequently as is considered necessary and practicable.

2.15. In the event that there are any significant and substantive changes to the nature of the interference and/or the identity of the equipment during the currency of the warrant, the Intelligence Services should consider whether it is necessary to apply for a fresh section 5 warrant.

General best practices

2.16. The following guidelines should be considered as best working practices by the Intelligence Services with regard to all applications for warrants covered by this code:

- applications should avoid any repetition of information;
- information contained in applications should be limited to that required by the 1994 Act;

- where warrants are issued under urgency procedures (see Chapter 4), 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;
- where it is foreseen that other agencies will be involved in carrying out the operation, these agencies should be detailed in the application; and
- warrants should not generally be sought for activities already authorised following an application by the same or a different public authority.

2.17. Furthermore, it is considered good practice that within each of the Intelligence Services, a *designated senior official* should be responsible for:

- the integrity of the process in place within the Intelligence Service to authorise equipment interference;
- compliance with the 1994 Act and this code;
- engagement with the Intelligence Services Commissioner when he or she conducts his inspections; and
- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by the Commissioner.

3. LEGALLY PRIVILEGED AND CONFIDENTIAL INFORMATION

Overview

3.1. The 1994 Act does not provide any special protection for 'confidential information'. Nevertheless, particular consideration should be given in cases where the subject of the operation might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information includes communications subject to *legal privilege*, communications between a Member of Parliament and another person on constituency business, confidential personal information, or confidential journalistic material. So, for example, particular consideration should be given where, through equipment interference comprising the obtaining of information, it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter's spiritual welfare, or between a Member of Parliament and a constituent relating to constituency business, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved. References to a Member of Parliament include references to a Member of the UK Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly, and to a UK member of the European Parliament.

Information subject to legal privilege

Introduction

3.2. Section 98 of the Police Act 1997 describes those matters that are subject to legal privilege in England and Wales. In relation to Scotland, those matters subject to legal privilege contained in section 33 of the Criminal Law (Consolidation) (Scotland) Act 1995 should be adopted. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

3.3. Legal privilege does not apply to communications or items held with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications or items will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use the information for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

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

3.5. Although the 1994 Act does not provide any special protection for legally privileged material, the acquisition of knowledge of matters 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 knowledge of matters subject to legal privilege (whether deliberate or otherwise) is therefore subject to additional safeguards under this code.

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

3.6. Any application for equipment interference that is likely to result in the acquisition of knowledge of matters subject to legal privilege (as described in paragraph 3.2) should include, in addition to the reasons why it is considered necessary for the equipment interference to take place, an assessment of how likely it is that communications which are subject to legal privilege will be acquired. In addition, it should state whether the purpose (or one of the purposes) of the equipment interference is to obtain knowledge of matters subject to legal privilege.

3.7. If the equipment interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege, but it is likely that such knowledge will nevertheless be acquired during the operation, that should be made clear in the warrant application and the application should identify the steps which will be taken to mitigate the risk of acquiring it. If the risk cannot be removed entirely, the application should explain what steps will be taken to ensure that any knowledge of matters subject to legal privilege which is obtained is not used in law enforcement investigations or criminal prosecutions. The application should also confirm that any inadvertently obtained communications that are 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 communications subject to legal privilege.

3.8. Where the intention of the equipment interference is to acquire knowledge of matters subject to legal privilege, the application should explain what steps will be taken to ensure that any knowledge of matters subject to legal privilege which is obtained is not used in law enforcement investigations or criminal prosecutions, and should also confirm that any communications that are 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 communications subject to legal privilege. The Secretary of State will only issue the warrant if satisfied that there are

exceptional and compelling circumstances that make the authorisation necessary. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb, or to national security, and the equipment interference is reasonably regarded as likely to yield intelligence necessary to counter the threat.

3.9. Further, in considering any equipment interference likely or intended to result in the acquisition of knowledge of matters subject to legal privilege, the Secretary of State must be satisfied that the proposed equipment interference is proportionate to what is sought to be achieved. In particular, the Secretary of State should consider whether the purpose of the proposed equipment interference could be served by obtaining non-privileged information. In such circumstances the Secretary of State will be able to impose additional conditions such as regular reporting arrangements, so as to be able to exercise his or her discretion on whether a warrant should continue to have effect.

3.10. Where there is a renewal application in respect of a warrant which has resulted in the obtaining of legally privileged material that fact ought to be highlighted in the renewal application.

Lawyers' communications

3.11. Where a lawyer is the subject of an investigation or operation, it is possible that a substantial proportion of the communications which will be acquired will be between the lawyer and his or her client(s) and will be subject to legal privilege. Therefore, and for the avoidance of doubt, in any case where a lawyer is the subject of equipment interference, the application should be made on the basis that it is intended to acquire communications subject to legal privilege and the provisions in paragraph 3.8 will apply, as relevant.

3.12. Any case where a lawyer is the subject of equipment interference should also be notified to the Intelligence Services 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, dissemination and deletion

3.13. Caseworkers who examine information obtained by equipment interference should be alert to any material which may be subject to legal privilege. Where there is doubt as to whether the information is subject to legal privilege, or as to the handling of such information, advice should be sought from a legal adviser within the relevant Intelligence Service. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception.

3.14. Material which has been identified as legally privileged should be retained only where it is necessary and proportionate to do so in accordance with the statutory functions of each of the Intelligence Services 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 statutory purposes.

3.15. Material subject to legal privilege should not be acted on or further disseminated unless a legal adviser has been consulted on the lawfulness (including the necessity and proportionality) of such action or dissemination.

3.16. The retention of legally privileged material, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to 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. 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 Intelligence Service, with any possible connection to the proceedings. In respect of civil proceedings, there can be no

circumstances under which it is proper for any of the Intelligence Services to seek to rely on legally privileged material in order to gain a litigation advantage over another party in legal proceedings.

3.17. In order to safeguard against any risk of prejudice or accusation of abuse of process, the Intelligence Services should also take all reasonable steps to ensure that (as far as practicable) lawyers or policy 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 relevant Intelligence Service should seek independent advice from Counsel and, if there is assessed to be a risk that such material could yield a litigation advantage, the direction of the Court.

3.18. In those cases where legally privileged material has been acquired and retained, the matter should be reported to the Intelligence Services Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any material that is still being retained should be made available to him or her if requested, including detail of whether that material has been disseminated.

3.19. For the avoidance of doubt, the guidance in paragraphs 3.1 to 3.18 takes precedence over any contrary content of an agency's internal advice or guidance.

Confidential information

3.20. Particular consideration should also be given to cases that involve confidential personal information, confidential constituent information and confidential journalistic material.

3.21. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his physical or mental health or to spiritual counselling.[11] Such

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

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 is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

3.22. 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.

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

3.24. Where the intention is to acquire confidential information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential information is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to adopting special handling arrangements within the relevant Intelligence Service.

3.25. Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so in accordance with the statutory functions of each of the Intelligence Services 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 statutory purposes.

3.26. Where confidential 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 handling and dissemination of confidential information, advice should be sought from a legal adviser within the relevant Intelligence Service before any further dissemination of the material takes place.

3.27. Any case where confidential information is retained should be reported to the Intelligence Services Commissioner as soon as reasonably practicable, as agreed with the Commissioner, and any material which has been retained should be made available to the Commissioner on request.

3.28. The Prime Minister must be consulted in any case where a Member of Parliament is subject to an investigation or operation utilising equipment interference techniques.

4. PROCEDURES FOR AUTHORISING EQUIPMENT INTERFERENCE UNDER SECTION 5

General basis for lawful activity

4.1. Subject to paragraph 4.4, a warrant under section 5 of the 1994 Act should be sought wherever members of the Intelligence Services, or persons acting on their behalf or in their support, conduct equipment interference in relation to equipment located in the British Islands that would be otherwise unlawful.

4.2. If the equipment is located outside the British Islands, and the interference would be otherwise unlawful, the Security Service should seek a warrant under section 5 of the 1994 Act. In the case of SIS and GCHQ, an authorisation under section 7 may be obtained instead of a warrant under section 5[12] (see chapter 8).

4.3. An application for a section 5 warrant should usually[13] be made by a member of the Security Service, SIS or GCHQ 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 SIS and GCHQ.

4.4. SIS and GCHQ may not be issued with a warrant for action in support of the prevention or detection of serious crime which relates to equipment in the British Islands. The Security Service may only be issued with a warrant for action in support of the prevention or detection of serious crime which relates to equipment in the British Islands if it authorises the taking of action in relation to conduct which would constitute one or more offences and:

12 This includes cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus: section 7(9). See also section 7(10) to (12).

13 Where two Intelligence Services are conducting *equipment interference* as part of a joint operation only one authorisation is required.

- It 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; or
- a person aged twenty-one or over with no previous convictions could reasonably be expected to be sentenced to three years' imprisonment or more.

4.5. In some cases an equipment interference operation may also enable or facilitate separate covert surveillance likely to result in the obtaining of private information about a person. A directed or intrusive surveillance authorisation may need to be obtained under Part 2 of the 2000 Act in such cases (see the Covert Surveillance and Property Interference Revised Code of Practice). Operations involving covert surveillance and equipment interference may be authorised as a combined warrant, although the criteria for authorisation of each activity should be considered separately.

Application for an equipment interference warrant

4.6. An application for the issue or renewal of a section 5 warrant is made to the Secretary of State.[14] Each application should contain the following information:

- the identity or identities, where known, of those who possess or use the equipment that is to be subject to the interference;
- sufficient information to identify the equipment which will be affected by the interference;
- the nature and extent of the proposed interference, including any interference with information derived from or related to the equipment;
- what the operation is expected to deliver and why it could not be obtained by other less intrusive means;
- details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected.

14 Warrants may be issued under section 5 by Scottish ministers in certain circumstances, by virtue of arrangements under the Scotland Act 1998. In this code references to the "Secretary of State" should be read as including Scottish ministers where appropriate. The functions of the Scottish ministers also cover renewal and cancellation arrangements.

- whether confidential or legally privileged material may be obtained. If the equipment interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege or confidential personal information, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it;
- details of any offence suspected or committed where relevant;
- how the authorisation criteria (as set out at paragraph 4.7 below) are met;
- what measures will be put in place to ensure proportionality is maintained (e.g. filtering, disregarding personal information);
- where an application is urgent, the supporting justification;
- any action which may be necessary to install, modify or remove software on the equipment including an assessment of the consequences (if any) of those actions;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results.

Issuing of section 5 warrants

4.7. Before issuing a warrant, the Secretary of State must:

- think it 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 a warrant 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 information obtained by means of the warrant, and that information obtained will be subject to those arrangements.

Urgent authorisation of a section 5 warrant

4.8. Section 6 of the 1994 Act makes provision for cases in which a warrant is required urgently, yet the Secretary of State is not available to issue the warrant. In these cases the Secretary of State will still personally authorise the equipment interference but the warrant is signed by a senior official, following discussion of the case between the senior official and the Secretary of State.

4.9. The 1994 Act restricts issue of warrants in this way to urgent cases where the Secretary of State has expressly authorised the issue of the warrant, and requires the warrant to contain a statement to that effect.

Renewals of warrants

4.10. A warrant, unless renewed, ceases 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).

4.11. 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, the Secretary of State may by an instrument under his hand renew it for a period of six months beginning with the day it would otherwise cease to have effect.

Cancellations of warrants

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

4.13. The person who made the application to the Secretary of State should apply for its cancellation, if they are satisfied that the warrant no longer meets the criteria upon which it was authorised.

Retrieval of equipment

4.14. Because of the time it can take to remove the means of interference it may also be necessary to renew an equipment interference warrant in order to complete the removal. Applications to the Secretary of State for renewal should state why the operation is being or has been closed down, why it has not been possible to remove the means of interference and any relevant timescales for removal.

5. KEEPING OF RECORDS

Centrally retrievable records of warrants

5.1. The following information relating to all section 5 warrants for equipment interference should be centrally retrievable for at least three years:

- all applications made for warrants and for renewals of warrants;
- the date when a warrant is given;
- whether a warrant is approved under urgency procedures;
- where any application is refused, the grounds for refusal as given by the Secretary of State;
- the details of what equipment interference has occurred;
- the result of periodic reviews of the warrants;
- the date of every renewal; and
- the date when any instruction was given by the Secretary of State to cease the equipment interference.

6. HANDLING OF INFORMATION AND SAFEGUARDS

Overview

6.1. This chapter provides further guidance on the processing, retention, disclosure deletion and destruction of any information obtained by the Intelligence Services pursuant to an equipment interference warrant. This information may include communications content and communications data as defined in section 21 of the 2000 Act.

The Intelligence Services should ensure that their actions when handling information obtained by means of equipment interference comply with the legal framework set out in the 1989 and 1994 Acts (including the arrangements in force under these Acts),[15] the Data Protection Act 1998 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 this legal framework will ensure that the handling of information obtained by equipment interference continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards against abuse.

Use of information as evidence

6.2. Subject to the provisions in chapter 3 of this code, information obtained through equipment interference may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984[16] and the 1998 Act.

15 All information obtained by equipment interference should be handled in accordance with arrangements made under section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act (and pursuant to sections 5(2)(c) and 7(3)(c) of the 1994 Act).

16 And section 76 of the Police and Criminal Evidence (Northern Ireland) Order 1989.

Handling information obtained by equipment interference

6.3. Paragraphs 6.6 to 6.11 provide guidance as to the safeguards which should be applied by the Intelligence Services to the processing, retention, disclosure and destruction of all information obtained by equipment interference.[17] Each of the Intelligence Services must ensure that there are internal arrangements in force, approved by the Secretary of State, for securing that these requirements are satisfied in relation to all information obtained by equipment interference.

6.4. These arrangements should be made available to the Intelligence Services Commissioner. The arrangements should ensure that the disclosure, copying and retention of information obtained by means of an equipment interference warrant is limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes set out in section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act. Breaches of these handling arrangements should be reported to the Intelligence Services Commissioner as agreed with him.

Dissemination of information

6.5. 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 proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. This obligation applies equally to disclosure to additional persons within an Intelligence Service, and to disclosure outside the service. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: information obtained by equipment interference should not be disclosed to any person unless that person's duties are

17 The application of these safeguards to all information obtained by *equipment interference* is without prejudice as to whether section 6 of the 1998 Act requires the application of these safeguards to information other than communications content and associated communications data.

such that they need to know about the information to carry out those duties. In the same way only so much of the information may be disclosed as the recipient needs; for example if a summary of the information will suffice, no more than that should be disclosed.

6.6. The obligations apply not just to the Intelligence Service that obtained the information, but also to anyone to whom the information is subsequently disclosed. In some cases this may be achieved by requiring the latter to obtain the originator's permission before disclosing the information further. In others, explicit safeguards may be applied to secondary recipients.

Copying

6.7. Information obtained by equipment interference may only be copied to the extent necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. Copies include not only direct copies of the whole of the information, but also extracts and summaries which identify themselves as the product of an equipment interference operation. The restrictions should be implemented by recording the making, distribution and destruction of any such copies, extracts and summaries that identify themselves as the product of an equipment interference operation.

Storage

6.8. Information obtained by equipment interference, and all copies, extracts and summaries of it, should be handled and stored securely, so as to minimise the risk of loss or theft. It should be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store such information securely applies to all those who are responsible for the handling of the information.

Destruction

6.9. Communications content, communications data and other information obtained by equipment interference, and all copies, extracts and summaries thereof, should be marked for deletion and securely destroyed as soon as they are no longer needed for the functions or purposes set out in paragraph 6.5. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

Personnel security

6.10. In accordance with the need-to-know principle, each of the Intelligence Services should ensure that information obtained by equipment interference is only disclosed to persons as necessary for the proper performance of the Intelligence Services' statutory functions. Persons viewing such product will usually require the relevant level of security clearance. Where it is necessary for an officer to disclose information outside the service, it is that officer's responsibility to ensure that the recipient has the necessary level of clearance.

7. APPLICATION OF THE CODE TO EQUIPMENT INTERFERENCE PURSUANT TO SECTION 7 OF THE 1994 ACT

Application of the code to other equipment interference

7.1. SIS and GCHQ should as a matter of policy[18] apply the provisions of this code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of the 1994 Act in relation to equipment located outside the British Islands.

7.2. This chapter provides specific additional guidance on certain aspects of the process for authorising equipment interference pursuant to section 7 of the 1994 Act. Save as specified below, GCHQ and SIS should comply with all other provisions of this code in relation to equipment interference under section 7. In particular, GCHQ and SIS should apply all the same procedures and safeguards when conducting equipment interference authorised pursuant to section 7 as they do in relation to equipment interference authorised under section 5.

General basis for lawful activity

7.3. An authorisation under section 7 of the 1994 Act may be sought wherever members of SIS or GCHQ, or persons acting on their behalf or in their support, conduct equipment interference in relation to equipment located outside the British Islands that would otherwise be unlawful. This includes cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus.[19]

18 And without prejudice as to arguments regarding the applicability of the ECHR.

19 See section 7(9).

7.4. If a member of SIS or GCHQ wishes to interfere with equipment located overseas but the subject of the operation is known to be in the British Islands, consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained in advance of commencing the operation authorised under section 7. In the event that any equipment located overseas is brought to the British Islands during the currency of the section 7 authorisation, and the act is one that is capable of being authorised by a warrant under section 5, the interference is covered by a 'grace period' of 5 working days (see section 7(10) to 7(14)). This period should be used either to obtain a warrant under section 5 or to cease the interference (unless the equipment is removed from the British Islands before the end of the period).

7.5. An application for a section 7 authorisation should usually[20] be made by a member of SIS or GCHQ for the taking of action in relation to that service. Responsibility for issuing authorisations under section 7 rests with the Secretary of State.

7.6. An authorisation under section 7 may be specific to a particular operation or user, or may relate to a broader class of operations. Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, *internal approval* to conduct operations under that authorisation in respect of equipment interference should be sought from a designated senior official (see paragraphs 7.11 to 7.14).

20 Where two Intelligence Services are conducting equipment interference as part of a joint operation only one authorisation is required.

Authorisations for equipment interference under section 7

7.7. An application for the giving or renewal of a section 7 authorisation is made to the Secretary of State. Each application should contain the same information, as far as is reasonably practicable in the circumstances, as an application for a section 5 equipment interference warrant.

7.8. Before giving the authorisation, the Secretary of State should be satisfied that:

- the equipment interference, or the operation in the course of which the equipment interference will take place, will be necessary for the proper discharge of a function of SIS or GCHQ;
- there are satisfactory arrangements in force to secure that nothing will be done beyond what is necessary for the discharge of SIS or GCHQ's functions and that the nature and likely consequences of any acts done in reliance on the authorisation will be reasonable having regard to the purposes for which they are carried out;
- there are satisfactory arrangements in force under the 1994 Act in respect of disclosure of any information obtained by means of the authorisation, and that any information so obtained will be subject to those arrangements.

Urgent authorisation of a section 7 authorisation

7.9. Section 7(5) of the 1994 Act makes provision for cases in which an authorisation is required urgently, yet the Secretary of State is not available to give the authorisation. In these cases the Secretary of State will still personally authorise the equipment interference but the authorisation is signed by a senior official, following discussion of the case between the senior official and the Secretary of State.

7.10. The 1994 Act restricts issue of authorisations in this way to urgent cases where the Secretary of State has expressly authorised the giving of the authorisation, and requires the authorisation to contain a statement to that effect.

Other authorisations and internal approvals

7.11. An authorisation under section 7 may relate to a broad class of operations. Authorisations of this nature are referred to specifically in section 7(4)(a) of the 1994 Act which provides that the Secretary of State may give an authorisation which inter alia relates to "acts of a description specified in the authorisation". The legal threshold for giving such an authorisation is the same as for a specific authorisation.

7.12. Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of equipment interference should be sought from a designated senior official. In any case where the equipment interference is likely or intended to result in the acquisition of confidential information, authorisation should be sought from an Annex A approving officer. Where knowledge of matters subject to legal privilege may be acquired, the Annex A approving officer should apply the tests set out at paragraph 3.4 to 3.7 (and "Secretary of State" should be read as "Annex A approving officer" for these purposes).

7.13. The application for approval should set out the necessity, justification, proportionality and risks of the particular operation, and should contain the same information, as and where appropriate, as an application for a section 5 equipment interference warrant. Before granting the internal approval, the designated senior official or Annex A approving officer should be satisfied that the operation is necessary for the proper discharge of the functions of the Intelligence Service, and that the taking of the action is proportionate to what the action seeks to achieve. The designated senior official or Annex A approving officer should consult the Foreign and Commonwealth Office or seek the endorsement of the Secretary of State for any particularly sensitive operations.

7.14. All internal approvals should be subject to periodic review at least once every 6 months to ensure the operations continue to be necessary and proportionate. The approvals for particularly sensitive operations should be reviewed more frequently, depending on the merits of the case.

Renewals of authorisations

7.15. A section 7 authorisation, unless renewed, ceases to have effect at the end of the period of six months beginning with the day on which it was given (if the authorisation was given 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 given (in any other case).

7.16. If at any time before the day on which an authorisation would cease to have effect the Secretary of State considers it necessary for the authorisation to continue to have effect for the purpose for which it was given, the Secretary of State may by an instrument under his hand renew it for a period of six months beginning with the day it would otherwise cease to have effect.

Cancellations of authorisations

7.17. The Secretary of State must cancel an authorisation if he or she is satisfied that any act authorised by it is no longer necessary.[21]

21 See section 7(8).

8. OVERSIGHT BY INTELLIGENCE SERVICES COMMISSIONER

8.1. The Intelligence Services Commissioner provides independent oversight of the use by the Intelligence Services of the powers contained within the 1994 Act. This code does not cover the exercise of any of the Commissioner's functions.

8.2. It is the duty of any member of the Intelligence Services who uses these powers to comply with any request made by the Commissioner to disclose or provide any information they require for the purpose of enabling him to carry out his functions. Such persons should also report any action that is believed to be contrary to the provisions of the 1994 Act to the Commissioner.

9. COMPLAINTS

9.1. The 2000 Act establishes an independent Tribunal (the Investigatory Powers Tribunal). This Tribunal will be made up of designated senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. This Code does not cover the exercise of the Tribunal's functions.

9.2. Details of the relevant complaints procedure are available on the Tribunal's website at: http://www.ipt-uk.com or can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

020 7035 3711

10. GLOSSARY

Confidential information

Confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege. See Chapter 3 for a full explanation.

Designated senior official

"Designated senior official" means a person holding at least the grade of Deputy Director with SIS or GCHQ and who has been designated for the purpose in question by (as relevant) the Chief of the SIS or the Director of GCHQ or their nominated deputies.

Equipment interference

Any interference (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf of in their support, with equipment producing electromagnetic, acoustic and other emissions, or information derived from or related to such equipment, which is to be authorised under section 5 of the 1994 Act, in order to do any or all of the following:

a) obtain information from the equipment in pursuit of intelligence requirements;

b) obtain information concerning the ownership, nature and use of the equipment with a view to meeting intelligence requirements;

c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);

d) enable and facilitate surveillance activity by means of the equipment;

"Information" may include communications content, and communications data as defined in section 21 of the 2000 Act.

Intelligence Services	The Security Service, SIS and GCHQ.
Internal approval	Internal approval given by a designated senior official to conduct operations under an authorisation relating to a broader class of operations given by the Secretary of State under section 7 of the 1994 Act.
Legal privilege	Matters subject to legal privilege are defined (as relevant) in section 98 of the Police Act 1997, section 33 of the Criminal Law (Consolidation) (Scotland) Act 1995 and Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989. This includes certain communications between professional legal advisers and their clients or persons representing the client.
Public authority	Any public organisation, including the Intelligence Services.
Secretary of State	Any Secretary of State (in practice this will generally be the Home Secretary in the case of the Security Service, and the Foreign Secretary in the case of SIS and GCHQ).

11. ANNEX A

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

Intelligence Service	Authorisation level
The Security Service	Deputy Director General
The Secret Intelligence Service	A Director of the Secret Intelligence Service
The Government Communications Headquarters	A Director of the Government Communications Headquarters

This code of practice provides guidance on the use by the Intelligence Services of section 5 of the Intelligence Services Act 1994 to authorise equipment interference to which the code applies. It provides guidance on the procedures that should be followed before equipment interference can take place under that provision, and on the processing, retention, destruction and disclosure of any information obtained by means of the interference.

Primarily intended for those members of the Intelligence Services involved in the use of equipment interference, the code will also be informative to others interested in the conduct of equipment interference.

tso
part of Williams Lea

www.tso.co.uk

ISBN 978-0-11-341394-2
9 780113 413942