These notes refer to the Regulation of Investigatory Powers Act 2000 (c.23) which received Royal Assent on 28 July 2000

REGULATION OF INVESTIGATORY POWERS ACT 2000

EXPLANATORY NOTES

INTRODUCTION

1. These explanatory notes relate to the Regulation of Investigatory Powers Act which received Royal Assent on 28 July 2000. They have been prepared by the Home Office in order to assist the reader in understanding the Act and have not been endorsed by Parliament.

2. The notes need to be read in conjunction with the Act. They are not, and are not meant to be, a comprehensive description of the Act. So where a section or part of a section does not seem to require any explanation or comment, none is given.

SUMMARY AND BACKGROUND

3. The main purpose of the Act is to ensure that the relevant investigatory powers are used in accordance with human rights. These powers are:

   - the interception of communications;
   - the acquisition of communications data (eg billing data);
   - intrusive surveillance (on residential premises/in private vehicles);
   - covert surveillance in the course of specific operations;
   - the use of covert human intelligence sources (agents, informants, undercover officers);
   - access to encrypted data.

4. For each of these powers, the Act will ensure that the law clearly covers:

   - the purposes for which they may be used;
   - which authorities can use the powers;
   - who should authorise each use of the power;
   - the use that can be made of the material gained;
   - independent judicial oversight;
   - a means of redress for the individual.

5. Not all of these matters need be dealt with in this Act – in many cases existing legislation already covers the ground. The Act will work in conjunction with existing legislation, in particular the Intelligence Services Act 1994, the Police Act 1997 and the Human Rights Act 1998.

OVERVIEW

6. The Act is in five parts.

Interception of Communications and the Acquisition and Disclosure of Communications Data

7. The existing arrangements for the interception of communications are established in the Interception of Communications Act 1985. Significant changes to that Act were proposed in the Consultation Paper "Interception of Communications in the United Kingdom" (CM 4368) published on 22 June 1999.

8. This Act repeals the 1985 Act and provides for a new regime for the interception of communications incorporating the changes proposed in the consultation paper. These changes go beyond what is strictly required for human rights purposes and provide also for the changed nature of the communications industry since 1985.

9. The provisions also implement Article 5 of Council Directive 97/66 of 15 December 1997, known as the "Telecommunications Data Protection Directive", which requires member states to safeguard the confidentiality of communications.

Surveillance and Covert Human Intelligence Sources

10. This Part provides a statutory basis for the authorisation and use by the security and intelligence agencies, law enforcement and other public authorities of covert surveillance, agents, informants and undercover officers. It will regulate the use of these techniques and safeguard the public from unnecessary invasions of their privacy.

Investigation of Electronic Data Protected by Encryption etc

11. This Part contains provisions to maintain the effectiveness of existing law enforcement powers in the face of increasing criminal use of encryption. Specifically, it will introduce a power to require disclosure of protected (encrypted) data.

12. The first consultation on this subject was undertaken by the previous administration in March 1997. A broader consultation "Building Confidence in Electronic Commerce: A Consultation Document" was launched on 5 March 1999 (URN 99/642). Finally, provisions very similar to these were published as Part III of the draft Electronic Communications Bill issued for consultation on 23 July 1999 (CM 4419).

Scrutiny of Investigatory Powers and Codes of Practice

13. This Part ensures that there will be independent judicial oversight of powers where necessary.

14. It also establishes a Tribunal as a means of redress for those who wish to complain about the use of the powers.

15. Finally, it provides for the Secretary of State to issue Codes of Practice covering the use of the powers covered by the Act.

Miscellaneous and Supplemental

16. This Part makes minor amendments to Wireless Telegraphy Act 1949, Part III of the Police Act 1997 in the light of operational experience and extends those provisions to the Ministry of Defence Police, the British Transport Police and the Service Police.

17. Both the Police Act 1997 and the Intelligence Services Act 1994 are amended to ensure authority is given for interference with property or wireless telegraphy only where it is proportionate to do so.

COMMENTARY ON SECTIONS

Section 1: Unlawful and authorised interception

18. This Section creates the offences of unlawful interception and a separate civil liability for unlawful interception, explains the locations and circumstances in which each is applicable, and the circumstances in which interception is lawful.

19. *Subsection (1)* sets out the circumstances in which interception of a communication being transmitted by a public postal service or public telecommunication system is a criminal offence. The offence is similar to that created by Section 1 of the Interception of Communications Act 1985, which this Act repeals.

"Public postal service" and "public telecommunication system" are defined in Section 2(1).

There is an exception for conduct with "lawful authority", as to which see subsection (5). For territorial limitation, see section 2(4).

20. *Subsection (2)* sets out the circumstances in which interception of a communication being transmitted by a private telecommunication system is an offence. The 1985 Act contains no equivalent of this offence. There is an exclusion for the circumstances set out in subsection (6), to which this subsection refers. However, interceptions in those circumstances give rise to a civil liability, as to which see subsection (3).

"Private telecommunication system" is defined in Section 2(1).

There is an exception for conduct with "lawful authority", as to which see subsection (5). For territorial limitation, see section 2(4).)

21. *Subsection (3)* creates civil liability for unlawful interception on a private telecommunications network, the locations at which the liability applies and the persons who may bring an action under this subsection, namely the sender, recipient or intended recipient. For example, where an employee believes that their employer has unlawfully intercepted a telephone conversation with a third party, either the employee or the third party may sue the employer.

There is an exception for conduct with "lawful authority", as to which see subsection (5). Particularly relevant to this liability are the regulations that may be made under Section 4(2). For territorial limitation, see section 2(4).

22. *Subsection (4)* applies to international agreements on mutual assistance in connection with the interception of communications which are designated under this subsection by an order made by the Secretary of State (negative resolution, see Section 78). This will enable the United Kingdom to comply with the interception provisions in the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. Although no similar agreements are currently under negotiation, this subsection will provide flexibility for the future.

23. In respect of agreements designated by this order, this subsection requires the Secretary of State to ensure that no request for mutual assistance to intercept communications, or in connection with interception, is made unless it has lawful authority. "Lawful authority" has the meaning given by subsection (5); in practice, for the purposes of the Convention referred to above, this means that the Secretary of State must issue an interception warrant under Section 5(1)(b) prior to any request for mutual assistance.

"International mutual assistance agreement" is defined in Section 20

24. *Subsection (5)* explains the circumstances in which interception of communications is lawful, and where the offences and the liability created in subsections (1), (2) and (3) do not therefore apply. These are where the interception is not authorised by an interception

warrant yet falls into one of the exceptions described in Sections 3 or 4 (for example where all parties to the communication consent to the interception); where there is an interception warrant; or where an existing statutory power is used in order to obtain stored communications. The latter case covers circumstances where, for example, a person has been arrested in possession of a pager, and the police have reason to believe that the messages sent previously to that pager may be of assistance in the case. In this case they would be able to seek from a circuit judge an order under Schedule 1 to the Police and Criminal Evidence Act 1984 for the stored data to be produced.

25. *Subsection (6)* explains the circumstances in which interception falls outside the scope of the criminal offence introduced by subsection (2). This conduct attracts civil liability by virtue of subsection (3). Essentially, subsection (6) allows a person with a right to control a private telecommunication network to intercept on their own network without committing an offence. Examples of this type of activity are an individual using a second handset in a house to monitor a telephone call, and a large company in the financial sector routinely recording calls from the public in order to retain a record of transactions. Each of those cases may or may not give rise to civil liability, depending on the application of sections 3 and 4.

26. *Subsection (7)* specifies the maximum penalties for the offences created by this section. The statutory maximum referred to in paragraph (b) is currently £5000. There is no upper limit to a fine on conviction in the Crown Court.

Section 2: Meaning and location of "interception" etc

27. This Section sets out the definitions of telecommunications and postal services and systems relevant to the Act, and assists in the interpretation of interception and other related matters. For the interpretation of other terms used in Chapter I of Part I, see sections 20 and 81.

"Private telecommunication system" is defined as any telecommunication system which is not a public telecommunication system; but is attached to such a system. This means that an office network, linked to a public telecommunication system by a private exchange, is to be treated as a private system. Interception of such a system other than by the system controller or with his consent is a criminal offence. An entirely self-standing system, on the other hand, such as a secure office intranet, does not fall within the definition.

28. *Subsection (2)* explains what constitutes the interception of a communication in the course of its transmission by means of a telecommunication system. This is relevant to the criminal offence and the civil liability in Section 1; and to the issuing of a warrant by the Secretary of State which authorises or requires interception in Section 5. There is no equivalent definition for postal interception.

"Wireless telegraphy" and "apparatus" are defined in Section 81.

For "while being transmitted", see subsection (7).

29. The exclusion in *subsection (3)* for communications broadcast for general reception covers television and radio. It does not extend to pager or mobile phone signals; the interception of those communications is governed by the Act.

30. *Subsection (4)* explains how the territorial limitation works in Section 1(1), (2) and (3), each of which extends only to interception "at any place in the United Kingdom".

31. *Subsection (5)* excludes from the definition of interception in subsection (2) any conduct which relates only to the traffic data comprised in or attached to a communication (expanded in subsection (9)), or which relates only to so much of the content of the communication as is necessary in order to identify this traffic data.

32. *Subsection (7)* expands the phrase "while being transmitted", which is used in the tailpiece of subsection (2). The times when a communication is taken to be in the course of its transmission include any time when it is stored on the system for the intended recipient to collect or access. This means that an interception takes place, for example, where an electronic mail message stored on a web-based service provider is accessed so that its contents are made available to someone other than the sender or intended recipient, or where a pager message waiting to be collected is accessed in that way. However, if a stored communication is accessed in this way, that conduct may be lawful by virtue of Section 1(5)(c).

33. *Subsection (9)* sets out the meaning of "traffic data". It covers, for example, subscriber information under paragraph (a), and routing information under paragraph (b). Paragraph (c), which must be read with subsection (10) (which operates on subsection (5)), addresses what is commonly referred to as "dial through fraud". It covers, for example, data entered by a user seeking to arrange for a telephone call to be accepted and routed by a telecommunication system. Finally, paragraph (d) catches the data which is found at the beginning of each packet in a packet switched network which indicates which communications data attaches to which communication. The tailpiece to the definition puts beyond doubt that in relation to internet communications, traffic data stops at the apparatus within which files or programs are stored, so the traffic data may identify a server but not a website or page.

34. The tailpiece to the definition puts beyond doubt that in relation to internet communications, traffic data stops at the apparatus within which files or programs are stored, so the traffic may identify a server but not a website or page.

35. In s*ubsection (10),* paragraph (a) is explained above. Paragraph (b) ensures that the references to data being attached to a communication in subsection (5) include data which may not be transmitted simultaneously with the contents of that communication; for example, the data which identifies the number of the person making a telephone call (the calling line identifier).

Section 3: Lawful interception without an interception warrant

36. This Section authorises certain kinds of interception without the need for a warrant under Section 5, namely where one or more parties to a communication have consented to the interception, conduct is in relation to the provision or operation of services, or conduct takes place with the authority of a person designated for the purposes of the Wireless Telegraphy Act 1949.

37. *Subsection (1)* authorises interception where there are reasonable grounds for believing that both the sender and the intended recipient of a communication have consented to its interception.

38. *Subsection (2)* authorises interception where:

- either the sender or intended recipient of a communication has consented to its interception; and
- the interception has been authorised under Part II (see Section 48(4)).

39. This situation might arise where a kidnapper is telephoning relatives of a hostage, and the police wish to record the call in order to identify or trace the kidnapper. The operation will be authorised as surveillance, rather than by means of an interception warrant.

40. *Subsection (3)* authorises interception where it takes place for the purposes of providing or operating a postal or telecommunications service, or where any enactment relating to the use of a service is to be enforced. This might occur, for example, where the postal provider needs to open a postal item to determine the address of the sender because the recipient's address is unknown.

41. *Subsection (4)* authorises interception where it is authorised by a designated person and is undertaken for purposes connected with certain parts of the Wireless Telegraphy Act 1949. Section 5 of that Act, as amended by Section 73 of this Act, makes provision for interception of wireless telegraphy under the Secretary of State's authority.

For "designated person", see Section 5(12) of the 1949 Act, inserted by Section 73.

Section 4: Power to provide for lawful interception

42. This Section lists the cases where a power may be exercised to provide for lawful interception without the need for a warrant under Section 5: under an international mutual assistance agreement; under regulations made by the Secretary of State to permit certain kinds of interception in the course of lawful business practice; under prison rules; in hospital premises where high security psychiatric services are provided; and in state hospitals in Scotland.

43. *Subsection (1)* enables the Secretary of State to make regulations specifying the conditions under which communication service providers may be authorised to use telecommunications systems located in the United Kingdom to intercept the communications of subjects on the territory of another country in accordance with the law of that country. The effect of paragraphs (d) and (e) is that regulations must be in operation before interception is authorised under this subsection. This subsection applies only where the subject of the interception is in the country whose competent authorities issued the interception warrant. The inclusion of the phrase "or who the interceptor has reasonable grounds for believing is in a country or territory outside the United Kingdom" reflects the fact that it will not always be possible to be certain about the precise location of the interception subject.

44. In practice, the "interceptor" is likely to be a communication service provider located in the UK which is either providing a public telecommunications service to another country or is in a business relationship with another communication service provider providing such a service.

45. This subsection will allow the United Kingdom to comply with Article 17 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. This Article is intended to allow operators of satellite communications systems to use a ground station in one Member State to facilitate interception using a "service provider" (in practice, a communications service provider which is in a business relationship with the satellite operator) located in another Member State. The "service provider" and the subject of interception are required to be in the same Member State.

46. *Subsection (2)* makes provision for the Secretary of State to make regulations describing the kinds of interception which it is lawful to carry out in the course of the carrying on of a business. Article 5 of Directive 97/66/EC (the Telecommunications Data Protection and Privacy Directive) exempts from its prohibition on interception.

""Any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication".

47. *Subsection (4)* makes reference to prison rules. Sections 47 and 39 of the respective Acts provide for the Secretary of State to make rules for the regulation and management of prisons and similar institutions, and for the classification, treatment, employment, discipline and control of people detained in them. The rules must, by virtue of section 6 of the Human Rights Act 1998, be compatible with the Convention rights.

For "prison", see subsection (9).

48. *Subsection (5)* makes reference to directions under section 17 of the National Health Service Act 1977. Under section 4 of that Act the Secretary of State has a statutory

duty to provide hospital services for persons who are liable to be detained under the Mental Health Act 1983 and in his opinion require treatment under conditions of high security on account of their dangerous, violent or criminal propensities. Under section 17 the Secretary of State may give directions to NHS bodies providing high security psychiatric services about their exercise of any functions. The directions must be compatible with Convention rights.

"High security psychiatric service" and "hospital premises" are defined in subsection (8)

49. *Subsection (6)* makes equivalent provision for the state hospitals in Scotland.

"state hospital" is defined in subsection (18)

Section 5: Interception with a warrant

50. This section allows for interception to be carried out when an interception warrant has been issued by the Secretary of State and sets out the grounds on which a warrant may be issued.

For "addressed" see section 7(3)

51. *Subsection (1)(a)* authorises the interception of communications sent by means of a postal service or telecommunication system.

"Interception" is described in Section 2.

52. *Subsection (1)(b)* allows the Secretary of State to issue an interception warrant for the purpose of making a request for assistance under an international mutual assistance agreement designated under Section 1(4).

53. *Subsection (1)(c)* allows the Secretary of State to issue an interception warrant for the purpose of complying with a request for assistance under an international mutual assistance agreement designated under Section 1(4).

54. *Subsection (1)(d)* allows for the disclosure of intercepted material and related communications data in a manner described by the warrant.

"Postal service" and "telecommunications system" are defined in Section 2(1).

"Related communications data", "intercepted material" and "international mutual assistance agreement" are defined in Section 20.

55. *Subsection (2)* requires that the Secretary of State may not issue an interception warrant unless he is satisfied that the warrant is necessary on grounds set out in subsection (3). *Subsection (2)(b)* introduces a proportionality test. Proportionality, under Convention case-law, is an essential part of any justification of conduct which interferes with an Article 8 right.

56. *Subsection (3)* sets out the grounds on which the Secretary of State may issue warrants. He may not do so unless he considers that the warrant is necessary on one of those grounds. It would not therefore be sufficient for him to consider that a warrant might be useful in supplementing other material, or that the information that it could produce could be interesting. The word 'necessary' reflects the wording of Article 8 of the Convention – "necessary in a democratic society".

57. *Subsection (3)(a)* "in the interests of national security" is the term used in Article 8 of the Convention. "National security" is not defined in the Act, as it is not in any other legislation in which it is used.

58. *Subsection (3)(b)* "for the purpose of preventing or detecting serious crime". This reflects the provision in Article 8 "for the prevention of disorder and crime", but is qualified by the word "serious".

"Serious crime" is defined in section 81(2) and (3)

"Detecting crime" is defined in section 81(5)

59. *Subsection (3)(c)* "for the purpose of safeguarding the economic well-being of the United Kingdom". This provision should be read in conjunction with Section 5(5) which introduces a significant limitation on its effect. Under Section 5(5) the Secretary of State is prevented from considering a warrant necessary under Section 5(3)(c) unless the information to be acquired under it is information relating to acts or intentions of persons outside the British Islands. A warrant could not therefore properly be issued in relation to purely domestic events. As with the other purposes for which interception is permitted, Section 5(3)(c) closely reflects the wording of Article 8 of the Convention, though the term in Article 8 is understood to have a broader meaning and would include, for example, the protection of tax revenues. The limitation imposed in Section 5(5) is not found in the Convention.

60. *Subsection (3)(d)* ensures that the Secretary of State will not issue an interception warrant for the purpose of an international mutual assistance agreement designated under Section 1(4) unless he is satisfied that the circumstances are equivalent to those in which he would issue a warrant for the prevention or detection of serious crime.

"International mutual assistance agreement" is defined in Section 20: it must be designated for the purposes of section 1(4).

61. *Subsection (4)* requires the Secretary of State to take account of other means of obtaining information when considering whether the requirements of subsection (2) are satisfied.

62. *Subsection (6)*(a) provides for the interception of such other communications (if any) as it is necessary to intercept in order to intercept the communications authorised by the warrant. This provides for situations where other communications are unavoidably intercepted in the course of intercepting the warranted communications.

63. *Subsection (6)(b)* allows for related communications data to be obtained during the course of interception. For example, this could cover the actions of a provider of communications services in effecting the requirements of a warrant where the intercepted material comprises both communications and related communications data.

64. *Subsection (6)(c)* allows for assistance in giving effect to the warrant to be provided to a person to whom the warrant is addressed; for example, by a person listed in Section 11(4).

Section 6: Application for issue of interception warrants

65. Section 6 describes the persons who may apply for warrants.

Section 7: Issue of warrants

66. Section 7 describes the persons who may sign interception warrants and the circumstances in which they may do so.

67. The combined effect of *subsections (1) and (2)* is that the warrant must be signed by the Secretary of State unless the case is either urgent or the purpose is to comply with a request for mutual assistance where the subject of the interception or the premises and the competent authority making the request are outside the United Kingdom.

68. In urgent cases a warrant may be signed by a senior official. The procedure in urgent cases has three elements:

- the senior official who signs the warrant must be expressly authorised by the Secretary of State to do so (under subsection (2(a)));
- that express authorisation must be in relation to that particular warrant (subsection (2)(a)); and
- under *subsection (4)(a)* the official who signs the warrant must endorse on it a statement that he has been expressly authorised by the Secretary of State to sign that particular warrant.

69. Thus, even where the urgency procedure applies, the Secretary of State must have given personal consideration to the application in order to give instructions to a senior official for the signing of that particular warrant, which will be limited in duration to five working days (see section 9(1) and (6)(a)).

"Senior official" is defined in Section 81(1).

"International mutual assistance agreement" is defined in Section 20.

70. *Subsection (2)(b)* allows an interception warrant to be issued under the hand of a senior official for the purpose of complying with a request for mutual assistance under an international mutual assistance agreement (designated under Section 1(4)) in circumstances in which the subject of the interception or the premises and the competent authority making the request are outside the United Kingdom.

71. This will allow the United Kingdom to comply with the requirements of Article 16 of the Convention on Mutual Assistance in Criminal Matters. Article 16 includes the situation where the United Kingdom is requested to issue an interception warrant to the operator of a satellite ground station in the United Kingdom for the purpose of intercepting a satellite telephone being used on the territory of another Member State. Article 16 enables such warrants to be issued by the requested Member State (in this case, the United Kingdom) "without further formality" provided the competent authorities of the requesting Member State have already issued an interception order against the subject of interception. Since no decision is being made on the merits of the case, and the purpose of the warrant is solely to require the satellite operator to provide technical assistance to the other Member State, it is considered appropriate for these warrants to be issued by senior officials rather than the Secretary of State.

72. *Subsection (3)* specifies to whom the warrant must be addressed (see list in Section 6(2)) and that in the case of a warrant under the hand of a senior official it contains one of the statements in subsection (4). The statement in subsection (4)(a) relates to urgent cases and is explained above.

73. *Subsection (4)(b)* applies only in cases where the warrant is issued in connection with a request made under an international mutual assistance agreement. It ensures, in conjunction with *subsection (5)*, that a statement of the purpose of the warrant is recorded, including the fact that it appears, at the time of the issue of the warrant, that the interception subject is outside the United Kingdom.

Section 8: Contents of warrant

74. This Section describes the two different forms which a warrant may take.

75. *Subsections (1)(a) and (b)* require that either the person or the set of premises to be intercepted is named or described on the face of the warrant.

"Person" is defined in Section 81(1).

"Interception" is described in Section 2.

76. *Subsections (2) and (3)* require that a warrant must include one or more schedules describing which communications are to be intercepted. The schedule or schedules will do this by setting out the addresses (for example, telephone numbers or e-mail addresses), numbers, apparatus or other factors, or combination of factors. By subsection (3), each factor or combination of factors must identify communications which are or are likely to include communications from or intended for the person described in the warrant, or originating on or intended for transmission to the premises named in the warrant.

"Communication" is defined in section 81(1).

77. *Subsection (4)* describes a second form which warrants may take. It applies if the conditions in subsections (4)(a) and (b), are met.

78. *Subsection (4)(a)* confines the conduct authorised or required by the warrant to conduct falling within subsection (5).

79. *Subsection (4)(b)* requires that at the time when the Secretary of State issues the warrant there must be in existence a certificate certifying the description of intercepted material the examination of which he considers necessary as is mentioned in section 5(3)(a), (b) or (c) – namely the purposes for the issue of warrants other than the one relating to international mutual assistance agreements. The effect of this subsection is to require the Secretary of State to authorise a certificate describing the intercepted material which falls properly within the purpose and may therefore be read, looked at or listened to by any person. No other intercepted material, though the communications are lawfully intercepted, may be so examined. The material authorised for examination is therefore subject to Ministerial control.

80. *Subsection (5)(a)* covers conduct that consists in the interception of communications in the course of their transmission by a telecommunication system. The effect of this is to limit warrants under this provision to telecommunication, and to exclude postal items. These communications must also be external communications, i.e. sent or received outside the British Islands.

"External communications" is defined in Section 20.

81. *Subsection (5)(b)* covers conduct authorised by an interception warrant by Section 5(6). See Explanatory Notes for Section 5(6)(a) to (c).

82. *Subsection (6)* requires a certificate to be issued under the hand of the Secretary of State. The control exercised through the certificate has therefore to be a personal Ministerial one. There is no provision for delegation of this power to officials, even in urgent cases.

Section 9: Duration, cancellation and renewal of warrants.

83. Section 9 provides for the issue, duration and renewal of warrants.

84. *Subsection (1)(a)* states that a warrant ceases to have effect at the end of the relevant period unless renewed under the power in subsection (1)(b). A renewal instrument must be issued under the hand of the Secretary of State unless the warrant was issued under Section 7(2)(b), in which case the renewal instrument may be issued by a senior official. Section 7(2)(b) applies to cases in which the warrant is issued to comply with a request for mutual assistance where the subject of interception or the relevant premises and the competent authority making the request are outside the United Kingdom.

"Relevant period" is defined in subsection (6).

"Working day" is defined in section 81(1).

85. *Subsection (2)* adds a condition that the Secretary of State may only renew a warrant under subsection (1) if he considers that the warrant continues to be necessary as mentioned in Section 5(3) (in the interests of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic well-being of the UK or for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement).

86. *Subsection (3)* requires the Secretary of State to cancel a warrant at any time if he considers that it is no longer necessary as mentioned in Section 5(3).

87. *Subsection (4)* requires the Secretary of State to cancel a warrant where the warrant or renewal instrument was issued under the hand of a senior official on the basis that the subject of the interception was outside the United Kingdom, but the Secretary of State is satisfied that the subject is now in the United Kingdom. For the interception to continue in such circumstances, a new warrant will need to be issued by the Secretary of State himself.

88. *Subsection (5)* applies to renewal instruments issued under the hand of a senior official for the purpose of renewing a warrant issued to comply with a request for mutual assistance where the subject of interception and the competent authority making the request are outside the United Kingdom. In such cases, the renewal instrument must contain a statement that the interception subject or the premises to which the interception relates are outside the United Kingdom.

89. *Subsection (6)(a)* applies to warrants issued under the urgency procedure in section 7(2)(a). Such warrants last for a maximum of five working days following the day of the warrant's issue. Thus a warrant issued in this way at any time on day one will expire at midnight on the fifth working day after day one. If renewed under the hand of the Secretary of State within five working days a warrant initially issued under the urgency procedure then falls within subsection (6)(c) and is valid for three months beginning with the day of the renewal.

90. Under s*ubsection (6)(b)* the relevant period is six months, beginning with the day of the warrant's renewal. The result of this is that warrants the renewal of which is considered necessary as mentioned in section 5(3)(a) (in the interests of national security) or (c) (for the purpose of safeguarding the economic well-being of the UK) lapse unless renewed by the Secretary of State within a period of six months.

91. Under s*ubsection (6)(c)* the relevant period is three months beginning with the day of the warrant's issue or, in the case of a warrant that has been renewed, of its latest renewal. The effect of this is that all new warrants, and all warrants the renewal of which is considered necessary as mentioned in section 5(3)(b) (for the purpose of preventing or detecting serious crime), are valid for three months from the day of the warrant's issue or renewal.

"International mutual assistance agreement" is defined in Section 20.

Section 10: Modification of warrants and certificates

92. Section 10 sets out the circumstances in which warrants and certificates may be modified and by whom this may be done.

93. *Subsection (1)(a)* gives the Secretary of State the power to modify the provisions of an interception warrant.

94. *Subsection (1)(b)* gives the Secretary of State the power to modify the description of interception material specified in a Section 8(4) certificate so as to include any material the examination of which he considers necessary for a purpose mentioned in Section 5(3)(a), (b) or (c) (in the interests of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic well-being of the UK).

95. *Subsection (2)* requires the Secretary of State to modify a schedule if at any time he considers that any factor in the schedule is no longer relevant for identifying communications from, or intended for, the person named or described in the warrant or the communications originating on or intended for transmission to the premises so named or described. The modification is to take the form of the deletion of the factor in question. This provision is the modification equivalent of the cancellation provision in Section 9(3).

96. *Subsection (3)* requires the Secretary of State to modify the description in a certificate if at any time he considers that it includes material the examination of which is no longer necessary for the purposes mentioned in section 5(3)(a) to (c). The modification is to take the form of the exclusion of the material in question.

97. *Subsection (4)* allows only the Secretary of State or a senior official to modify a warrant or certificate subject to subsections (5) to (8).

98. By s*ubsection (5),* a senior official may only modify the unscheduled parts (explained in subsection (10) below) of an interception warrant in an urgent case where the official is expressly authorised by the Secretary of State himself to make the modification and a statement of that fact is on the modifying instrument. This is the same as the urgency procedure for the issue of warrants.

99. The restriction in subsection (5) does not apply to the scheduled parts of a warrant, which may therefore be modified without each modification being referred personally to the Secretary of State. Such modifications shall be valid for five working days – see subsection (9). But s*ubsection (6)* restricts the senior officials who may modify the scheduled parts of a warrant by prohibiting those listed in Section 6(2) or their subordinates from making modifications under this provision. The intention is that this function will only be exercised by senior officials in the department of a Secretary of State.

100. *Subsection (7)* requires that a senior official may only modify a section 8(4) certificate in an urgent case where the official is expressly authorised by the provisions contained in the certificate to modify the certificate on the Secretary of State's behalf or the Secretary of State has expressly authorised the modification and a statement of that fact is on the modifying instrument. Again such modifications shall be valid for five working days – see subsection (9).

101. *Subsection (8)* is a separate power to that provided by subsection (4). It permits the persons listed in Section 6(2) or any of their subordinates, where they are expressly authorised by the warrant, to make urgent modifications to the scheduled parts of an interception warrant. Again such modifications shall be valid for five working days – see subsection (9).

"Working day" is defined in Section 81(1).

102. *Subsection (10)* explains what is meant by modifying the scheduled or unscheduled parts of an interception warrant.

Section 11: Implementation of warrants

103. This Section addresses the question of how an interception warrant may be implemented once it has been authorised, and the role of different people within this process.

104. *Subsection (1)* allows the interception to be carried out either by the person to whom the warrant is addressed (ie where it is technically feasible, by the intercepting agency itself), or by other persons providing assistance in the implementation.

For "provide assistance", see subsection (9).

105. *Subsection (2).* Where an intercepting agency requires another person to assist it in implementing an interception, it is likely that the person providing assistance will wish to be satisfied that there is an interception warrant in existence. This subsection provides for this, allowing the intercepting agency to provide either a copy of the warrant or to make arrangements whereby a copy is provided.

106. *Subsection (3).* Where a copy of a warrant is served upon a person providing assistance in accordance with subsection (2), this subsection allows the intercepting agency to restrict the disclosure of the warrant to just that material which the person providing assistance needs to see in order to satisfy themselves that their actions are authorised. Most commonly this may involve a communications service provider only being shown the front of the warrant (showing the name of the person to be intercepted) and the specific schedule which identifies the communications which they are being asked to provide assistance in intercepting.

107. *Subsection (4)* states that where a person providing a communications service is required to give assistance in accordance with an interception warrant, they must do everything required of them by the person to whom the warrant is addressed in order to give effect to the warrant. As to what the warrant authorises or requires, see Section 5.

108. *Subsection (5)* ensures that no unreasonable demands are made of service providers.

109. *Subsection (6)* explains that that where a service provider has had an obligation to provide an intercept capability imposed upon them under Section 12, it is reasonable to expect them to be able to provide assistance with an intercept up to the level of the imposed capability.

110. *Subsection (7)* creates a criminal offence of knowingly failing to comply with a requirement to provide the required assistance in implementing an interception warrant. It goes on to specify the maximum penalties which a person who is found guilty of this offence may be sentenced to. On the statutory maximum, see the note for Section 1(7).

111. *Subsection (8)* also allows the Secretary of State to take civil proceedings against a person who fails to provide the required assistance under subsection (4) in order to compel him to provide such assistance by means of, inter alia, an injunction or other appropriate relief.

112. *Subsection (9)* explains that the term "provision of assistance" includes the actual disclosure of the intercepted material and related communications data to the person to whom the warrant is addressed (or his representative).

Section 12: Maintenance of interception capability

113. This section provides a power allowing the Secretary of State to impose obligations upon providers of publicly available communication services to maintain a reasonable intercept capability.

114. *Subsection (1)* provides the mechanism by which the Secretary of State may set out a framework for obligations upon persons providing or planning to provide public postal services or public telecommunications services. The Secretary of State will do this through an order (affirmative resolution, see subsection (10)) which lays out the obligations which he believes are reasonable, with the aim of ensuring that providers are capable of giving assistance in the implementation of interception warrants. The order itself will not impose specific requirements on providers but will describe in general terms the kind of intercept capability which they may be required to provide.

For the meaning of "public postal service" and "public telecommunications service", see Section 2(1). But see also Section 12(4), which limits the application of this section.

115. *Subsection (2)* explains that the Secretary of State imposes obligations on particular providers by the service of individual notices describing in much greater detail than the order the precise steps they are required to take.

As to what steps may be imposed, see subsections (3) and (11). For the time limits for compliance, see subsection (8).

116. *Subsection (4)* provides that commercial and other organisations which provide a telecommunications service as no more than a means of accessing a further service of theirs (for example, a telephone banking service) will not be subject to any order under this section. The subsection also puts outside the scope of the section a telecommunications service that is necessarily incidental to a different service.

117. *Subsections (5) and (6)* concern the consideration of notices by the Technical Advisory Board (established by Section 13(1)). Where a person is served with a notice under subsection (2), they may ask the Board to consider the notice. The Board will consider the technical requirements and financial consequence of the notice, and report their conclusions to the person on whom the notice was served and to the Secretary of State. During that time, the obligations under the notice are suspended by virtue of paragraph (a). The Secretary of State, on receipt of advice from the Board, may withdraw the notice or re-issue it with or without modifications.

118. *Subsection (7)* requires persons served with a notice under subsection (2) to comply with it. The Secretary of State may bring civil proceedings to enforce this duty.

119. *Subsection (9)* requires the Secretary of State to consult with a number of people prior to making an order. These include, as the Secretary of State considers appropriate, the persons likely to have obligations imposed on them and their representatives, the Technical Advisory Board, and bodies which have statutory functions affecting providers of communication services. The latter category includes, for example, OFTEL.

120. *Subsection (11)* explains that the steps that may be required to be taken should take account of the need for security and confidentiality and the need to facilitate (such as by audit mechanisms) the job of the Interception Commissioner.

Section 13: Technical Advisory Board

121. This Section provides for the establishment by order of a Technical Advisory Board. Its make-up will be prescribed by order (affirmative resolution – see subsection (3)), and must include a balanced representation of the interests of communications service providers and of those people listed in section 6(2).

Section 14: Grants for interception costs

122. This Section requires the Secretary of State to ensure that there are arrangements to secure that communications service providers receive such a contribution as is fair in each particular case to the costs of providing an intercept capability or in the provision of assistance in respect of individual warrants.

Section 15: General safeguards

123. This Section has the effect of restricting the use of intercepted material to the minimum necessary for the authorised purposes. Section 82(6) contains a transitional provision applying the provisions of Sections 15 and 16 to warrants and certificates under the 1985 Act.

124. *Subsection (1)* imposes a duty upon the Secretary of State to ensure that safeguard arrangements are in place to ensure the requirements of this section and section 15 are complied with.

125. *Subsection (2)* requires that the distribution and disclosure of intercepted material and related communications data are kept to a minimum.

126. *Subsection (3)* requires that all copies of any intercepted material and related communications data must be destroyed as soon it is no longer necessary to retain it for any of the authorised purposes (see below). This does not impose any obligation to retain material, which may therefore be destroyed earlier in some cases.

"Copy" is defined in subsection (8).

127. *Subsection (4)* defines "authorised purposes", which are the reasons which determine the extent of distribution and disclosure allowed under subsection (2) and the reasons for which intercepted material may be retained rather than being destroyed under subsection (3).

128. *Subsection (5)* requires that intercepted material and related communications data are stored in a secure manner for as long as they are retained.

129. *Subsections (6) and (7)* apply where possession of intercepted material or related communications data has been surrendered to any authorities of a country or territory outside the United Kingdom. Possession may be surrendered in this way where an interception warrant has been issued for the purpose of complying with a request under an international mutual assistance agreement designated under Section 1(4). For example, where such a request results in the provision of intercept material by the communication service provider to the competent authorities of another country in real-time, the material will not, at any point, be under the control of an intercepting agency in the United Kingdom.

130. For these reasons, the Secretary of State will be required to make such arrangements (if any) corresponding to subsections (2) and (3) as he thinks fit. The Secretary of State will also be required to ensure, to such extent (if any) as he thinks fit, that restrictions are in force preventing the disclosure in any proceedings outside the United Kingdom which could not be made in the United Kingdom by virtue of Section 17 (the exclusion of intercept material from legal proceedings).

Section 16: Extra safeguards in the case of certificated warrants

131. This Section creates extra safeguards in addition to those provided in Section 15, in the case of warrants to which Section 8(4) certificates apply.

132. *Subsections (1) and (2)* provide the additional safeguards which apply. Material intercepted under the authority of a warrant to which a certificate applies should only be examined if it:

- has been certified as necessary to be examined in the interests of national security; for the purpose of preventing or detecting serious crime; or for the purpose of safeguarding the economic well-being of the United Kingdom; and
- does not have as its purpose, or one of its purposes, the identification of material contained in communications sent by, or intended for, an individual who is known to be for the time being in the British Islands; and
- has not been selected by reference to such an individual.

133. *Subsection (3)* provides an exception to the second and third criteria above where under a Section 8(4) certificate the Secretary of State has certified that material selected by reference to such an individual is necessary for one of the three purposes outlined above.

This material may only relate to communications sent during the period specified in the certificate; and the period specified must not be more than three months.

134. *Subsections (4), (5) and (6)* provide two further exceptions where:

- the person to whom the warrant is addressed believes on reasonable grounds both that the material examined is not referable to an individual known to be in the British Islands, and that the material has not been selected for the purpose of identifying material contained in communications sent by, or intended for, such an individual; or
- it has appeared to the person to whom the warrant is addressed that circumstances have changed such that the individual concerned has entered the British Islands, or that their belief in the individual's absence from the British Islands was mistaken; and since it first so appeared, written authorisation to examine the material has been given by a senior official.

135. The senior official may only provide authorisation until the end of the first working day after the day on which the change of circumstances became apparent.

Section 17: Exclusion of matters from legal proceedings

136. Section 17, subject to certain exceptions, prohibits evidence, questioning or assertion in (or for the purposes of, or in connection with) legal proceedings likely to reveal the existence or absence of a warrant. A similar provision is contained in section 9 of the Interception of Communications Act 1985, which this Act repeals.

137. *Subsection (1)* imposes the basic prohibition. It does this directly, by stating that the contents of intercepted material and associated communications data may not be disclosed, and indirectly by prohibiting the disclosure of any suggestion that actions under subsection (2) have occurred.

138. *Subsection (2)* describes the actions which may not be disclosed, including actions by persons named in subsection (3) which would constitute offences under this Act or section 1 of the 1985 Act.

139. *Subsection (3)* lists the people referred to in subsection (2)(a). They are people who may be in possession of information about authorised interception. In paragraph (3)(b) persons holding office under the Crown includes constables and, by virtue of Section 81(6), Crown servants and members of the Armed Forces.

Section 18: Exceptions to section 17

140. *Subsections (1)* and (3) list the proceedings in relation to which the prohibition in section 17(1) will not apply. None of the exceptions make anything admissible that would, but for the Act, be inadmissible. The exceptions merely remove the prohibition imposed by Section 17.

"Relevant offence" is explained in subsection (12).

141. *Subsection (2)* prevents the disclosure of information mentioned in section 17(1) to certain categories of person involved in proceedings before the Special Immigration Appeals Commission and the Proscribed Organisations Appeal Commission.

142. *Subsection (4)* allows the disclosure of the contents of a communication if the interception was lawful without the need for a warrant by virtue of Sections 1(5)(c), 3 or 4. This means that interception carried out in those circumstances may be evidential.

143. *Subsection (7)* allows the disclosure of the fact and contents of an interception to a person conducting a criminal prosecution. A prosecutor has a duty, recognised in case-law, to ensure that a prosecution is conducted fairly. This provision allows the intercepting agency to give the prosecutor access to any intercept material which has

not been destroyed so that he can discharge that duty effectively. This subsection further provides that the fact and contents of an interception may also be disclosed to a relevant judge in exceptional circumstances (see subsection (8) below). The subsection allows disclosure to the judge alone.

"Relevant judge" is explained in subsection (11).

144. *Subsection (8)* makes it clear that the judge must be satisfied that the exceptional circumstances of the case make any disclosure under subsection (7)(b) essential in the interests of justice.

145. *Subsection (9)* provides for a relevant judge where he has ordered disclosure under subsection (7)(b) in exceptional circumstances to direct the person conducting the prosecution in any criminal proceedings to make any such admission of fact as that judge thinks is essential in the interests of justice.

146. *Subsection (10)* makes it clear that a judge cannot order an admission of fact in contravention of Section 17(1). The admission, therefore, must be one that does not tend to suggest that an interception has taken place.

Section 19: Offence for unauthorised disclosures

147. This section places a requirement upon specified groups of persons to keep secret all matters relating to warranted interception.

148. *Subsection (2)* describes the groups of persons upon whom there is a duty to keep secret matters relating to warranted interception. These include:

- anyone to whom an interception warrant may be addressed. These are described in Section 6 and include both heads of intercepting agencies but also anyone who may make an application for an interception warrant on their behalf;
- anyone holding office under the Crown (civil servants, police officers and members of Her Majesty's forces) and civilian employees of police authorities;
- anyone providing or employed for the purpose of providing either a postal service or a public telecommunications service;
- anyone controlling any part of a telecommunications system in the United Kingdom.

149. *Subsection (3)* describes the matters which must be kept secret. In essence these are anything to do with the existence or implementation of a warrant, including the content of the intercepted material and related communications data.

150. *Subsection (4)* creates the offence of unlawful disclosure and specifies the maximum penalties which a person who is found guilty of the criminal offence of unlawful disclosure may be sentenced to; if he is found guilty in a Magistrates' Court he may be imprisoned for a period up to six months or fined up to the statutory maximum (currently £5000) or both; in a Crown Court he may be imprisoned for a period up to five years, or may be fined (no upper limit), or both.

151. *Subsection (5)* gives a defence where a person could not reasonably have been expected to take steps to prevent the unlawful disclosure.

152. *Subsections (6) and (7)* give further defences to the offence of unlawful disclosure and addresses the question of a person consulting their legal adviser about requirements placed upon them under this Act, and disclosures which their legal adviser may be required to make as a result of such consultation. For example, where a communications service provider is required to provide assistance with the implementation of an interception warrant, the provider may wish to first consult their lawyer. *Subsection (6)* provides a defence to such a consultation being an unlawful disclosure.

153. *Subsection (8)* places a limitation on the defences described in subsections (6) and (7), stating that the defences are not valid where a disclosure was made with a view to furthering any criminal purpose.

154. *Subsection (9)* gives a further defence to the offence of unlawful disclosure, stating that where such a disclosure was authorised in any of the ways described in this subsection this would constitute a defence.

Section 20

155. Section 20 interprets terms used in this Chapter.

"External communications": under the Interpretation Act 1978, the term "British Islands" means the United Kingdom, the Isle of Man and the Channel Islands. The use of the term in this Chapter therefore means that communications sent between the UK and the Islands, or between the Channel Islands and the Isle of Man, are not treated as external.

"Related communications data": the term "communications data" is defined for the purposes of Chapter II in Section 21(4).

Chapter Ii

156. This Chapter provides a legislative framework to cover the requisition, provision and handling of communications data. It explains the duties and responsibilities placed upon each party involved in these processes and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights.

Section 21: Lawful acquisition and disclosure of communications data

157. This Section explains the scope of this Chapter, the meaning of the term "communications data", and ensures that provision of communications data under these provisions fully meets the requirements of Article 8.

158. *Subsection (1)* draws a distinction between interception of communications in the course of their transmission, which is activity excluded from this part of the Act, and conduct involving the obtaining of or disclosure of communications data, which is activity covered by this part of the Act.

159. *Subsections (2)* and *(3)* have the effect of making the provision of communications data under this Chapter lawful. This ensures that there is no liability attached to actions undertaken as a result of a requirement or authorisation under this Chapter.

"Relevant enactment" is defined in subsection (5)

160. *Subsection (4)* explains what "communications data" means. In essence, it includes information relating to the use of a communications service but makes clear that this does not include the contents of the communication itself. The first part of the definition refers to traffic data comprised in or attached to a communication. The same term is used in Section 2(5).

Section 22: Obtaining and disclosing communications data.

161. This Section explains the purposes for which communications data may be sought under this Chapter and the arrangements by which such data may be required.

162. *Subsection (1)* explains that the strict test of "necessity" must be met before any communications data is obtained under this Chapter. The assessment of necessity is one made by a person designated for the purposes of this Chapter (defined in Section 25(2)).

163. *Subsection (2)* explains the reasons for which communications data may be required. With the exception of (g), these are the same as the purposes for which directed

surveillance and the use of a covert human intelligence source may be permitted by Sections 28 and 29 of the Act.

164. *Subsections (3)* and *(4)* describe the two ways in which communications data may be obtained. Firstly, subsection (3) provides a means for a designated person to authorise someone within the same relevant public authority (see Section 25(1)). This provides a legal basis upon which the public authority may collect the communications data themselves. For example, if a private telecommunications operator was technically unable to collect certain communications data, this subsection would provide the authority to allow an investigating body to collect the data themselves.

165. *Subsection (4)* provides the second way in which communications data may be obtained, where the designated person serves a notice upon the holder of the data, requiring them to comply with the terms of the notice.

166. *Subsection (5)* introduces a proportionality test. The designated person must not only consider the communications data to be "necessary" (subsection (1)) but must also consider the conduct involved in obtaining the communications data to be "proportionate".

167. *Subsection (6)* requires a communications service provider in receipt of a notice under subsection (4) above to comply with it as soon as is reasonably practicable.

168. *Subsection (7)* provides that a holder of data will not be required to supply data unless it is reasonably practicable to do so.

169. *Subsection (8)* explains that if a communications service provider fails to provide the required communications data then the Secretary of State may take civil proceedings against them, which may result in the issue of, inter alia, an injunction which would have the effect of compelling the provision of data.

Section 23: Form and duration of authorisations and notices

170. This section specifies the way in which authorisations and notices must be completed and their duration.

171. *Subsections (1) and (2)* explain the format which authorisations and notices must take.

172. *Subsection (3)* restricts the persons to whom the data may be disclosed to the person giving the notice or another specified person who must be from the same relevant public authority.

173. *Subsection (4)* explains that disclosure may only be required of data in the possession of, or obtained by the communications service provider during the authorisation period of authorisations and notices, which is set at one month.

174. *Subsections (5) and (6)* permit an authorisation or notice to be renewed at any period during the month, by following the same procedure as in obtaining a fresh authorisation or notice.

175. *Subsection (7)* explains that the period for which a renewed authorisation or notice is extant begins at the point at which the notice or authorisation it is renewing expires.

176. *Subsection (8)* requires the cancellation of a notice as soon as it is clear that the reasons for which it was granted are no longer valid.

Section 24: Arrangements for payments

177. This section allows for payment arrangements to be made in order to compensate holders of communications data for the costs involved in complying with notices issued under this Chapter.

Section 25: Interpretation of Chapter II

178. This section defines the terms used in the Chapter dealing with communications data.

179. *Subsection (2)* explains that the Secretary of State will identify the "persons designated for the purposes of this Chapter" in an order (negative resolution, see section 78). Under s*ubsection (3)*, he may place restrictions on who may act under these provisions and in what circumstances.

Part Ii: Surveillance and Covert Human Intelligence Sources

Introductory

180. This Part of the Act creates a system of authorisations for various types of surveillance and the conduct and use of covert human intelligence sources. In common with other Parts of the Act, the provisions themselves do not impose a requirement on public authorities to seek or obtain an authorisation where, under the Act, one is available (see section 80). Nevertheless, the consequences of not obtaining an authorisation under this Part may be, where there is an interference by a public authority with Article 8 rights and there is no other source of authority, that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Section 26: Conduct to which Part II applies

181. This section describes and defines the conduct that can be authorised under this Part of the Act. Three types of activity are covered: "directed surveillance", "intrusive surveillance" and the conduct and use of covert human intelligence sources.

182. "Directed surveillance" is defined in *subsection (2)* as covert surveillance that is undertaken in relation to a specific investigation or a specific operation which 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); and 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 this Part to be sought for the carrying out of the surveillance. By subsection (9), surveillance will be covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place. Directed surveillance may also include the interception of communications where there is no interception warrant and where the communication is sent by or is intended for a person who has consented to the interception *(section 48(4))*.

183. "Intrusive surveillance" is defined in *subsections (3)* to *(5)* as covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle. This kind of surveillance may take place by means either of a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside.

184. For these purposes, a private vehicle is one used primarily for private purposes, for example for family, leisure or domestic purposes (section 48(1)). *Subsection (4)* provides that surveillance is not intrusive when the device is one that only provides information about the location of the vehicle (eg a tracking device).

185. *Subsection (6)* provides that surveillance carried out by means of apparatus designed or adapted for the purpose of detecting the installation or use of a television receiver is neither directed nor intrusive.

186. *Subsection (8)* defines a "covert human intelligence source".

187. *Subsection (10)* defines "private information", in relation to a person, as including any information relating to his private or family life.

Authorisation of surveillance and human intelligence sources

Section 27: Lawful surveillance etc

188. This section provides that all conduct defined in section 26 will be lawful, provided it is carried out in accordance with the authorisation to which it relates. Authorised conduct may cover any action taken either in the UK or abroad.

189. Furthermore, there will be no civil liability arising out of conduct that is incidental to the authorised conduct. However, this is only the case where the incidental conduct should not have been separately authorised either under this Act or under existing legislation.

Section 28, 29 and 30: Authorisation of directed surveillance; Authorisation of covert human intelligence sources; and Persons entitled to grant authorisations under sections 28 and 29

190. These sections deal with the scheme of authorisations for directed surveillance and the conduct and use of covert human intelligence sources.

191. Section 30 provides that the persons entitled to grant such authorisations will be such persons within the relevant public authorities that are designated by order of the Secretary of State. In this respect, the relevant public authorities are specified in Parts I and II of Schedule 1. *Subsections (5) and (7)* allow the Secretary of State to add, remove, or move public authorities between Parts I and II of the Schedule. Adding authorities to the Schedule and moving an authority from Part II to Part I of the Schedule is subject to affirmative resolution.

192. *Subsection (2)* provides that where an authorisation for directed surveillance or the use or conduct of a covert human intelligence source is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State.

193. Police and Customs authorisations may only be granted on an application from within the force or authority in question (see section 33(1) and (2)).

194. Section 28 and 29 provide that authorisations cannot be granted unless specific criteria are satisfied, namely, that the person granting the authorisation believes that:

- the authorisation is necessary on specific grounds; and
- the authorised activity is proportionate to what is sought to be achieved by it.

195. The specific grounds are that the authorisation is necessary:

- in the interests of national security;
- for the purpose of preventing or detecting crime or 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;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
- for other purposes which may be specified by order of the Secretary of State.

196. In addition, there are two further criteria in relation to covert human intelligence sources: namely that specific arrangements exist to ensure that, amongst other things,

the source is independently managed and supervised, that records are kept of the use made of the source, that the source's identity is protected from those who do not need to know it, and that arrangements also exist to satisfy such other requirements as may be imposed by order made by the Secretary of State. The responsibility for the management and supervision of a source falls to specified individuals within the organisation benefiting from the use of the source. As there may be cases where a source carries out activities for more than one organisation, it is provided that only one organisation will be identified as having responsibility for each requirement in relation to such arrangements and record-keeping.

197. Section 29(7) provides that the Secretary of State may prohibit, by order, certain conduct/uses of covert sources altogether and enables him, in other specific cases, to impose additional requirements which must be satisfied before an authorisation may be granted.

198. *Subsection (*3) of section 30 provides that the Secretary of State may impose, by order, restrictions on the types of authorisations granted and on the circumstances or purpose for which such authorisations may be granted.

199. Sections 28(4) and 29(4) set out the conduct that is authorised by the authorisation. Broadly speaking, it covers any conduct that occurs whilst carrying out the specified surveillance or is comprised in the activities involving the specified conduct or use of a covert human intelligence source, provided it is carried out or takes place in the manner and for the purposes described.

Section 31: Orders under section 30 for Northern Ireland

200. Section 31 provides for the Office of the First Minister and Deputy First Minister, to be able to make an order specifying which authorities, with devolved functions in Northern Ireland, can lawfully authorise directed surveillance and the conduct and the use of covert human intelligence sources.

INTRUSIVE SURVEILLANCE

Section 32: Authorisation of intrusive surveillance

201. This section deals with authorisations for intrusive surveillance. Such authorisations may only be granted by the Secretary of State (see sections 41 and 42) and by senior authorising officers as defined in *subsection (6)*. Sections 33(3) and (4) provide that a senior authorising officer may not grant an authorisation, except on an application by a member of his/her force, Service, Squad or organisation.

202. Again, intrusive surveillance authorisations cannot be granted unless specific criteria are satisfied, namely that, the Secretary of State or senior authorising officer believes that:

- the authorisation is necessary on specific grounds; and
- the authorised activity is proportionate to what is sought to be achieved by it.

203. An additional factor which must be taken into account when considering whether the requirements are satisfied, is whether the information which it is thought necessary to obtain by the authorised conduct could reasonably be obtained by other means.

204. The specific grounds in this case are that it is necessary:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- in the interests of the economic well-being of the United Kingdom.

Police and customs authorisations

205. Sections 33 to 40 only apply to intrusive surveillance authorisations for investigations carried out by the police, NCIS, the National Crime Squad and Customs & Excise. They outline very similar procedures to those set out in part III of the Police Act 1997 (interference with property and wireless telegraphy).

Section 33: Rules for grant of authorisations

206. In the case of a police force, NCIS and the National Crime Squad, *subsection (3)* restricts an authorisation for intrusive surveillance involving residential premises to being granted only where the premises are within the area of operation of that force, Service or Squad. The areas of operations are set out in *subsection (6)*. For the three service police forces, this is defined in *subsection (7)*, in terms of the persons who are subject to "service discipline".

Section 34: Grant of authorisations for intrusive surveillance in the senior officer's absence

207. Where an application is made for an intrusive surveillance authorisation and the case is urgent but it is not reasonably practicable for the application to be considered by the "senior authorising officer" (as defined in section 32) or his designated deputy, an authorisation may be granted by a person entitled to act in his/her absence. *Subsection (4)* lists the officers entitled so to act and *subsection (6)* sets down those officers entitled to act as "designated deputies".

Section 35:Notification of authorisations for intrusive surveillance

208. Where a police or customs intrusive surveillance authorisation is granted, renewed or cancelled, except where it is cancelled under section 37(3), written notification must be given to an ordinary Surveillance Commissioner as soon as reasonably practicable. *Subsection (2)* requires that notification to be in accordance with arrangements made by the Chief Surveillance Commissioner and must specify the matters prescribed by order of the Secretary of State. Such a notice will indicate that the authorisation or renewal requires the approval of an ordinary Surveillance Commissioner before it takes effect (see section 36) or it will state that the case is one of urgency, together with the grounds for that belief. Although the order by the Secretary of State will be subject to the affirmative procedure, the initial order can be made without the approval of both Houses of Parliament, provided it is approved by Parliament within 40 days.

209. *Subsection (4)* provides that the ordinary Surveillance Commissioner will, as soon as practicable, scrutinise the notice, which can be transmitted by electronic means, and decide whether or not to approve the authorisation in those cases where his approval is required.

Section 36: Approval required for authorisations for intrusive surveillance to take effect

210. Except in urgent cases, authorisations granted for intrusive surveillance will not take effect until they have been approved by an ordinary Surveillance Commissioner and written notice of the Commissioner's decision has been given to the person who granted the authorisation.

211. Where the person who granted the authorisation believes the case to be one of urgency, the authorisation will take effect from the time of grant, provided the appropriate notice is given to the ordinary Surveillance Commissioner, as described in section 36(3).

212. *Subsection (4)* provides that an ordinary Surveillance Commissioner shall give his approval only if he is satisfied that there are reasonable grounds for believing that the

authorisation is necessary and that the surveillance is proportionate to what is sought to be achieved.

213. If an ordinary Surveillance Commissioner decides not to approve an authorisation, *subsection (5)* requires him to make a report of his findings to the "most senior relevant person" (as defined in *subsections (6) and (7)*). This will be the chief constable or equivalent.

Section 37: Quashing of police and customs authorisations for intrusive surveillance etc

214. This section gives Surveillance Commissioners the power to quash or cancel an authorisation for intrusive surveillance.

215. Under *subsection (2)*, an ordinary Surveillance Commissioner may quash an authorisation, with effect from the time of the grant of the authorisation or renewal, if he believes that the criteria for authorisation in section 32 were not met at the time the authorisation was granted or renewed.

216. Alternatively, he may, under *subsection (3)* cancel an authorisation if he believes that there are no longer any reasonable grounds for believing that the criteria in section 32 are met. In such a case, he may cancel the authorisation from the time that the criteria, in his opinion, ceased to be met.

217. If an authorisation was granted or renewed by way of the urgency procedure, and the ordinary Surveillance Commissioner is satisfied that, at the time of grant or renewal, there were no reasonable grounds for believing the case to be one of urgency, he may quash the authorisation.

218. He may also, under *subsections (5) and (6)*, order the destruction of records, apart from those required for pending civil or criminal procedures. Where an authorisation is cancelled, he may only order the destruction of records from the time the authorisation no longer meets the criteria specified in section 32.

219. An order to destroy records does not become operative until after the period allowed for appealing against the decision or the dismissal of such an appeal.

220. Where an ordinary Surveillance Commissioner exercises a power conferred by this section, he will make a report of his actions, together with his reasons, as soon as reasonably practicable, to the most senior relevant person (usually the chief constable) and to the Chief Surveillance Commissioner.

Section 38: Appeals against decisions by Surveillance Commissioners

221. A senior authorising officer, or a designated deputy or other person granting an intrusive surveillance authorisation in the absence of the senior authorising officer, may appeal to the Chief Surveillance Commissioner against:

- a refusal of a Surveillance Commissioner to approve an authorisation or renewal;
- a decision by a Surveillance Commissioner to quash or cancel an authorisation;
- a decision to make an order for the destruction of records.

222. *Subsection (*4) provides that the Chief Surveillance Commissioner must allow an appeal if:

- he is satisfied that the criteria set out in section 32 were met at the time in question; and
- he is not satisfied that the urgency procedure has been abused.

223. In relation to appeals against decisions to quash or cancel authorisations, the Chief Surveillance Commissioner may modify the decision if he considers that there were grounds for the action which the Surveillance Commissioner has taken but such action should have taken effect at a different time. In such cases, he may modify the Surveillance Commissioner's decision to that which he considers should have been made.

224. Where an appeal against a decision to quash or cancel an authorisation is allowed, *subsection (6)* provides that the Chief Surveillance Commissioner shall quash any related order for the destruction of records.

Section 39: Appeals to the Chief Surveillance Commissioner: supplementary

225. Where the Chief Surveillance Commissioner has determined an appeal, *subsection (1)* requires him to give notice of his determination to:

- the person who brought the appeal; and
- the ordinary Surveillance Commissioner whose decision was appealed against.

226. Where the appeal is dismissed, he will report his findings, to the appellant, the ordinary Surveillance Commissioner and to the Prime Minister. Other than this report, he will not give any reasons for his determination.

227. In accordance with section 107 of the Police Act 1997, the Chief Surveillance Commissioner will make an annual report on the discharge of his functions to the Prime Minister and may make a report to him at any other time of any matter relating to those functions (S*chedule 4, paragraph 8(10)*).

228. *Subsection (3)* provides that the annual reporting provisions contained in subsections (3) and (4) of the Police Act 1997 also relate to reports made by the Chief Surveillance Commissioner under subsection (2).

OTHER AUTHORISATIONS

229. Sections 41 and 42 also relate to intrusive surveillance authorisations, but deal with those granted by the Secretary of State.

Section 41: Secretary of State authorisations

230. *Subsection (*1) provides that the Secretary of State shall not grant such authorisations unless an application is made by a member of the intelligence agencies (Security Service, Secret Intelligence Service and GCHQ), an official of the Ministry of Defence, the Armed Forces, or a specified individual within a public authority designated for this purpose by order of the Secretary of State (*subsection (3)*). Such an order would be subject to the affirmative procedure. For these purposes, the three service police forces are not treated as members of the armed forces (*subsection (7)*); instead, their use of intrusive surveillance is regulated, in the same way as other police forces, by sections 33 to 40.

231. The effect of *subsection (2)* is that authorisations will only be granted to an official of the Ministry of Defence or a member of the Armed Forces, where it is necessary in the interests of national security or for preventing or detecting serious crime.

232. This section also provides the power for the Secretary of State to impose, by order, restrictions on designated public authorities for the carrying out of intrusive surveillance, on the circumstances in which, or the purposes for which, such authorisations may be granted, and on the persons who can make such an application.

Section 42: Intelligence services authorisations

233. Where the Secretary of State grants an authorisation to one of the intelligence services under this Part (which will be for intrusive surveillance, or intrusive surveillance combined with directed surveillance), the authorisation will take the form of a warrant. This is consistent with section 5 of the Intelligence Services Act 1994.

234. *Subsection (2)* provides that a single warrant may combine an authorisation for intrusive surveillance with an intelligence services warrant (defined in subsection (6): a property warrant under section 5 of the Intelligence Services Act 1994).

235. In addition to the requirements in section 32, *subsection (3)* limits SIS and GCHQ to obtaining a warrant for intrusive surveillance in the British Islands to investigations carried out in the interests of national security or the economic well-being of the UK. *Subsections (4) and (5)* enable the Security Service to act on behalf of SIS and GCHQ in applying for and granting any authorisation in connection with a function of SIS or GCHQ, provided that SIS or GCHQ would have the power to act in that way, and provided that it does not relate to the functions of SIS or GCHQ in support of the prevention or detection of serious crime.

Grant, renewal and duration of authorisations

Section 43: General rules about grant, renewal and duration

236. This section sets out the general rules for authorisations, including their granting, renewal, and duration.

237. *Subsection (1)* provides that, in urgent cases, an authorising officer may give an oral authorisation. All other authorisations must be in writing.

238. A single authorisation may be given, combining two or more authorisations under this part. When this occurs, the provisions of this Part which relate to one type of activity only shall apply to those parts of the authorisation which authorises that type of activity. Further provisions for combined authorisations are in section 33(5), 42(2) and 44(7).

239. Oral authorisations and those granted by officers entitled to act in urgent cases in the absence of the authorising officer or his designated deputy will expire after 72 hours, beginning with the time when the grant or renewal of an authorisation takes effect.

240. Except where granted or renewed orally or by an officer entitled to act in urgent cases, authorisations for the conduct or the use of covert human intelligence sources will last for 12 months, beginning with the day on which the grant or renewal takes effect.

241. In all other cases (except those made under the special provisions for the intelligence services contained in section 44), the authorisation will last for 3 months, beginning with the day on which the grant or renewal takes effect.

242. *Subsection (4)* provides that an authorisation may be renewed at any time before it ceases to have effect by any person entitled to grant a new authorisation of the same type. The same conditions attach to a renewal of surveillance as to the original authorisation. However, before renewal of an authorisation for the use or conduct of a covert human intelligence source, *subsection (6)* requires there to be a review of the use made of that source, the tasks given to that source and the information so obtained.

243. *Subsection (8)* enables the Secretary of State, by order, to provide that certain authorisations will cease to have effect after a shorter period of time than is otherwise provided for.

244. *Subsection (9)* clarifies the time from which a grant or renewal of an authorisation takes effect. It synchronises the duration of authorisations with those given for interference with property.

Section 44: Special rules for intelligence services authorisations

245. This section sets out special provisions in relation to authorisations granted to or by the intelligence services.

246. Under *subsection (1),* a warrant for intrusive surveillance or a renewal of such a warrant will not be issued except under the hand of the Secretary of State. However, in an urgent case, where the Secretary of State has personally authorised it, a warrant can be signed (but not renewed) by a senior official. This is the same urgency procedure as is provided in section 7(2)(a) for interception. Where this has happened, such a warrant will cease to have effect at the end of the second working day following its issue, unless renewed under the hand of the Secretary of State.

247. *Subsections (4) and (5)* relate to the authorisation of warrants for the intelligence services and for the authorisations and renewal of authorisations for directed surveillance where the authorisation is necessary in the interests of national security or in the interests of the economic well-being of the UK. Such warrants or authorisations last for a period of six months. Where this is a renewal, the period will start on the day when the previous authorisation or warrant would have expired. This is consistent with the provisions of the Intelligence Service Act 1994.

248. *Subsection (6)* enables the Secretary of State, by order, to provide that certain authorisations will cease to have effect after a shorter period of time than is otherwise provided for.

Section 45: Cancellation of authorisations

249. *Subsection (1)* sets out when the person who granted or renewed an authorisation must cancel it.

250. *Subsection (2)* sets out who else is responsible for cancelling the authorisation eg the person who would have granted it if it had not been an urgent case or been granted by a deputy. However, an authorising officer's deputy (defined in *subsections (6) and (7))* is also under a duty to cancel an authorisation in those cases where he would have had the power to grant the authorisation on the authorising officer's behalf.

251. *Subsections (4)* and (*5)* provide for the Secretary of State to make regulations setting out how the duty for cancelling authorisations should be performed where the authorising officer is no longer available, and on whom such a duty should fall.

Section 46: Restrictions on authorisations extending to Scotland

252. This section prevents the granting or renewal of an authorisation under this Part for activity by a public authority in Scotland if all the conduct authorised is likely to take place in Scotland, unless the authorisation is one for which the Act is (under subsection (2)) the relevant statutory provision. Thus it does not prevent:

- those seeking authorisation on the grounds of it being in the interests of national security or the economic well-being of the UK;
- the intelligence agencies;
- the Ministry of Defence, the Ministry of Defence Police or HM Armed Forces;
- Customs and Excise;
- the British Transport Police; or
- any other public authority named by order as having authority for all parts of the UK;

from obtaining an authorisation under this Act notwithstanding that all the conduct might take place in Scotland.

Supplemental provision for Part II

Section 47: Power to extend or modify authorisation provisions

253. The Secretary of State may, by order, change the types of activities which fall within the category of directed surveillance by providing that a type of directed surveillance will be treated as intrusive surveillance. Furthermore, he may, by order, provide that additional types of surveillance, which are not at present defined as directed or intrusive surveillance in section 26, will be covered by the Act and become capable of being authorised under Part II.

Section 48: Interpretation of Part II

254. This section gives interpretations for the terms used in this Part. Amongst other things, it gives an interpretation for "surveillance" and clarifies that this does not include references to:

- the use of a recording device by a covert human intelligence source to record any information obtained in the presence of the source (*subsection (3)(a) and (b)*);
- activity involving interference with property or wireless telegraphy which requires authorisation or warrant under section 5 of the Intelligence Services Act 1994 or Part III of the Police Act 1997 (subsection (3)(c).

Part Iii: Investigation of Electronic Data Protected by Encryption Etc

Section 49: Notices requiring disclosure

255. This section introduces a power to enable properly authorised persons (such as members of the law enforcement, security and intelligence agencies) to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information which they lawfully hold, or are likely to, in an intelligible form.

Intelligible is defined in section 56(3)

256. *Subsection (1)* limits the information to which this power to serve notices applies. It does so by defining the various means by which the protected information in question has been, or is likely to be, lawfully obtained. By way of illustration, this could be material:

- seized under a judicial warrant (e.g. under the Police and Criminal Evidence Act 1984 (PACE));
- intercepted under a warrant personally authorised by the Secretary of State under Chapter I of Part I of this Act;
- lawfully obtained under an authorisation given under Chapter II of Part I or Part II of this Act;
- lawfully obtained by an agency under their statutory functions but not under a warrant (e.g. under the Customs and Excise Management Act 1979); or
- which has lawfully come into the possession of an agency but not by use of statutory functions (e.g. material which has been voluntarily handed over).

257. *Subsection (2)* states that persons with the "appropriate permission" (see Schedule 2) may serve a notice imposing a disclosure requirement in respect of the protected information in question if there are reasonable grounds for believing:

- that the key to the relevant protected information is in the possession of the person on whom the notice is being served;

- that serving a notice imposing a disclosure requirement is necessary for the reasons set out in subsection (3), or necessary for securing the effective exercise or proper performance of any statutory power or duty of a public authority;
- that imposing a disclosure requirement is proportionate to what is sought to be achieved by doing so; and
- that an intelligible version of the relevant protected information cannot be obtained by any other reasonable means.

key is defined in section 56(1)

possession of a key is defined in section 56(2)

258. *Subsection (4)* explains the format which notices must take.

259. The effect of *subsections (5) and (6)* is that, where applicable, notices must be served on a senior officer within a corporate body or firm.

Senior officer is defined in section 49(10)

260. *Subsection (7)* states that the requirement in subsections (5) and (6) does not apply where there are special circumstances to the case which mean that the purposes for which a notice is given would be defeated if it was served on a senior officer in an organisation (e.g. where that senior officer is a suspect in a criminal investigation).

261. *Subsection (8)* specifies the persons to whom a disclosure may be made by the recipient of a notice.

262. *Subsection (9)* ensures that a key which has been used solely for the purpose of generating electronic signatures does not have to be disclosed in response to a notice.

electronic signature is defined in section 56(1)

263. The effect of Schedule 2, which is introduced by s*ubsection (11)*, is to set authorisation levels (described in Schedule 2) for permission to serve a notice under section 49. The level of authority required will vary depending on the power under which the protected information was, or is likely to be, lawfully obtained.

Section 50: Effect of notice imposing disclosure requirement

264. This section explains the effect of serving a notice imposing a disclosure requirement in various circumstances.

265. *Subsection (1)* applies where a person has, at the time a notice is served, possession of the relevant protected information and a means of accessing it and of disclosing it in an intelligible form. This means that they have the password, in the case of material protected by a password; or the decryption key in the case of encrypted material; or both, in the case of material protected in both ways. In these circumstances, the effect of imposing a disclosure requirement is, first, that the recipient of a notice may use any key in their possession to access the information or to put it into intelligible form; and, second, that they must disclose it in accordance with the terms of the notice.

266. *Subsection (2)* allows a person who is required to disclosure information in an intelligible form to instead disclose a relevant key if they so choose to do so.

267. The effect of*Subsection (3)* is that where a notice is served on a person who does not have the relevant protected information in their possession; or cannot access the information without use of a key which is not in their possession; or the notice contains a direction that a key must be disclosed (as to which, see section 51), that person must disclose any key to the information that is in their possession at a relevant time. But this duty is qualified by subsections (4) to (6).

268. The Act does not prevent the person giving a section 49 notice from giving the recipient access to the protected information, in order to allow then to produce plain text rather than disclose a key.

Relevant time is defined in section 50(10)

269. The effect of *Subsections (4) and (5)* is that where a person served with a notice is entitled or obliged to disclose a key, they need only provide those keys which are sufficient to access the relevant information and to put it into intelligible form. And *Subsection (6)* further provides that such a person may choose which keys to provide, so long as they suffice to access the information and render it intelligible.

270. *Subsection (7)* requires a person served with a notice to disclose every key to the relevant protected information that is in their possession, subject to the provisions in subsections (5) and (6). It means that a person need only provide those keys which suffice to access the information and render it intelligible, and that they may choose which keys to provide to achieve that end.

271. The effect of Subsection (8) is that where a person served with a notice no longer possesses a key to the relevant protected information, they are to disclose all information that is in their possession that would facilitate the discovery of the key.

Section 51: Cases in which key required

272. This section sets out the extra tests to be fulfilled if a key is required to be disclosed rather than the disclosure of protected information in an intelligible form.

273. *Subsection (1)* states that a notice may not contain a statement that it can be complied with only by disclosing a key unless a direction to this effect has been given by the person giving permission for the notice to be served.

274. The effect of *Subsections (2) and (3)* is that a direction that a key must be disclosed given by the police, HM Customs and HM Forces must be given expressly by a person of the rank set out in this subsection (namely, Chief Officer of police or equivalent).

275. *Subsection (4)* provides that a person may only give a direction requiring the disclosure of a key if he believes that there are special circumstances to the case making this necessary; and that giving such a direction is proportionate to what is sought to be achieved by doing so.

276. *Subsection (5)* specifies that in deciding whether it is proportionate to require that a key be disclosed, consideration must be given to the sort of other information also protected by the key in question and any potential adverse impact on a business that might result from requiring that a key be disclosed.

277. The effect of *Subsections (6) and (7)* is that any direction to disclose a key given internally by the police, HM Customs or HM Forces must be notified, within 7 days, to the Intelligence Services Commissioner or the Chief Surveillance Commissioner, as appropriate.

Section 52: Arrangements for payments for disclosure

278. This section allows for payment arrangements to be made in order to compensate persons required to disclose information following service of a notice under section 49.

279.

Section 53: Failure to comply with a notice

280. This section creates an offence of failing to comply with the terms of a notice served under section 49.

281. *Subsection (1)* states that a person served with a notice is guilty of an offence if he knowingly fails to comply with the disclosure requirement contained in that notice.

282. The effect of *Subsections (2) and (3)* is that in proceedings against a person for an offence under this section, where it is shown that a person has been in possession of a key, that can lead to a conviction, but only if the person fails to raise some doubt as to whether he still had the key when the notice was given.

283. *Subsection (4)* allows a defence to a person who shows that it was not practicable to comply with the disclosure requirement placed upon him by the time he was required to do so but that he did what was required as soon as was reasonably practicable.

284. *Subsection (5)* specifies the maximum sentence for the offence of failing to comply with a notice. As regards financial penalties, there is no upper limit to fines set in the Crown Court (on conviction on indictment). In a Magistrates Court (on summary conviction) the maximum fine is £5,000.

Section 54: Tipping-off

285. This section creates an offence where the recipient of a notice (but only one which explicitly contains a secrecy requirement), or a person that becomes aware of it, tips off another that a notice has been served, or reveals its contents. This is designed to preserve, where necessary, the covert nature of an investigation by, for example, a law enforcement agency. It outlines various statutory defences.

286. *Subsection (1)* limits this offence to occasions where the notice served explicitly demands secrecy.

287. *Subsection (2)* specifies that the inclusion of a secrecy requirement in a notice must be authorised by the person giving permission for such a notice to be served (or where such a person has himself permission to serve a notice - e.g. a Superintendent in certain cases).

288. *Subsection (3)* places restrictions on the instances when such a requirement may be imposed.

289. *Subsection (4)* specifies the maximum sentence for the tipping-off offence. On conviction in the Crown Court, the maximum term of imprisonment is five years. The financial penalties are as for the offence set out in section 53.

290. *Subsection (5)* provides a defence where the tipping-off occurred entirely as a result of software designed to give an automatic warning that a key had been compromised and where, in addition, the defendant was unable to stop this from taking place after receiving the notice.

291. *Subsections (6)* and *(7)* provide a defence where a disclosure is made to or by a professional legal adviser as part of advice about the effect of the provisions of this part of the Act given to a client or his representative; or where a disclosure was made by a legal adviser in connection with any proceedings before a court or tribunal.

292. The effect of *Subsection (8)* is that the protection in Subsections (6) and (7) will not apply where a professional legal adviser tips off a client with a view to furthering any criminal purpose.

293. *Subsection (9)* provides a statutory defence where the disclosure is made to a Commissioner or authorised by:

- a Commissioner;
- the terms of the notice;
- the person who gave the notice, or someone on his behalf; or

- a person who is in possession of the data to which the notice relates, as described in section 49.

294. The effect of Subsection (9) is to ensure that, for example, persons within an organisation may be informed about a notice in order to give effect to the notice (e.g. accessing a key or plain text) without this falling foul of the tipping off offence.

295. *Subsection (10)* provides a statutory defence for a person told about a notice but not about the fact that there was a requirement for secrecy.

Section 55: General duties of specified authorities

296. This section describes the safeguards that must be in place for the protection of any material (e.g. a decryption key) handed over in response to the serving of a notice under this Act.

297. *Subsection (1)* ensures that the safeguard requirements apply to all those who may have responsibility for organisations that will handle material provided in response to a written notice. In the case of the security and intelligence agencies for example, this will mean the Secretary of State.

298. *Subsection (2)* places an onus on those identified to ensure that:

- any material disclosed is used only for a purpose for which it may be required;
- the uses to which the material is put are reasonable;
- the use and any retention of the material are proportionate;
- the requirements of subsection (3) are complied with;
- that keys are stored in a secure manner; and
- the material is destroyed as soon as it is no longer needed.

299. *Subsection (3)* specifies that the material is shared with the minimum number of people possible.

300. *Subsection (4)* imposes a civil liability in instances where seized keys are compromised by a failure of the safeguards arrangements in this section. There are two elements to this. Subsection (4)(a) is in respect of a person who fails to ensure that adequate arrangements are in place for the protection of keys. Subsection (4)(b) applies to where a person does not comply with those arrangements properly and compromises a key.

301. *Subsection (5)* describes the persons who may bring an action under the terms of this section. These are limited to persons who have made a disclosure in pursuance of a notice under section 49 or those whose protected information or key has been disclosed by some other person in pursuance of a notice.

Section 56: Interpretation of Part III

302. This section provides for the interpretation of various terms used in Part III of the Act.

Part Iv: Scrutiny Etc of Investigatory Powers and of the Functions of the Intelligence Services

Commissioners

Section 57: Interception of Communications Commissioner

303. This Section provides for the appointment of an Interception of Communications Commissioner to replace the Commissioner appointed under the Interception of Communications Act 1985. This is currently Lord Justice Swinton Thomas.

304. *Subsection (2)* details the remit of the Interception Commissioner. This will involve reviewing:

- the Secretary of State's role in interception warrantry;
- the operation of the regime for acquiring communications data;
- any notices for requiring the decryption of data authorised by the Secretary of State which relate to intercepted material or communications data;
- the adequacy of the arrangements made by the Secretary of State for the protection of intercepted material and by those persons listed in Section 55 for the protection of encryption keys for intercepted material and communications data.

305. *Subsection (7)* requires the Secretary of State to provide the Interception Commissioner with sufficient technical facilities and staff, after consultation with him. The provision itself places no limitation on the number of staff and (subject to Treasury approval as to numbers) allows flexibility over the numbers, grades and individuals.

306. *Subsection (8)* is a transitional provision allowing the existing Interception Commissioner to take office as the new Interception Commissioner on the coming into force of this section.

Section 58: Cooperation with and reports by s. 57 Commissioner

307. *Subsection (1)* requires that all those who may be involved in requesting, authorising, or carrying out, interception should cooperate with the Interception Commissioner as he reviews the operation of the regime.

308. *Subsection (3)* provides that the Interception Commissioner should report to the Prime Minister if he believes that arrangements made by the Secretary of State are inadequate for the protection of either intercepted material or decryption keys.

Section 59: Intelligence Services Commissioner

309. This Section provides for the appointment of an Intelligence Services Commissioner to replace the Commissioners appointed under the Security Service Act 1989 and the Intelligence Services Act 1994. Both posts are currently held by Lord Justice Simon Brown.

310. *Subsection (2)* details the remit of the Intelligence Services Commissioner.

311. *Subsection (7)* requires the Secretary of State to provide the Intelligence Services Commissioner with staff, after consultation with him. The provision itself places no limitation on the number of staff and (subject to Treasury approval as to numbers) allows flexibility over the numbers, grades and individuals.

312. *Subsection (9)* is a transitional provision allowing the existing Intelligence Service Act Commissioner to take office as the new Intelligence Services Commissioner on the coming into force of this section.

Section 61: Investigatory powers Commissioner for Northern Ireland

313. This section provides for the appointment of an Investigatory Powers Commissioner for Northern Ireland.

314. *Subsection (2)* details the remit of this Commissioner

Section 62: Additional functions of Chief Surveillance Commissioner

315. This Section allocates oversight of certain powers in this Act to the existing Chief Surveillance Commissioner established under the Police Act 1997.

316. It adds to the existing remit of the Chief Surveillance Commissioner the functions of reviewing the use of surveillance, agents, informants, undercover officers and decryption notices, and the arrangements for protecting decryption keys, so far as these are not required to be kept under review by any of the other Commissioners mentioned in this Act.

Section 63: Assistant Surveillance Commissioners

317. This section allows for the appointment of Assistant Surveillance Commissioners to help the Chief Surveillance Commissioner fulfil his duties. Assistant Surveillance Commissioners can be circuit judges or equivalent.

Section 64: Delegation of Commissioners' functions

318. This Section allows Commissioners to delegate statutory powers or duties to members of staff.

Section 65: The Tribunal

319. This Section establishes a Tribunal, sets out its jurisdiction and gives effect to Schedule 3, which provides for its constitution and functioning.

320. *Subsections (2) to (8)* set out the key elements of the Tribunal's jurisdiction. It is to be the appropriate forum for complaints or proceedings in relation to the following categories:

- any proceedings for actions incompatible with Convention rights which are proceedings against any of the intelligence services or people acting on their behalf; or which concern the use of investigatory powers under this Act, any entry on or interference with property, any interference with wireless telegraphy; where any of these take place in relation to conduct by any of the public authorities listed in subsection (6);
- any complaint by a person who believes that he has been subject to any use of investigatory powers under this Act, any entry on or interference with property, any interference with wireless telegraphy which he believes to have been carried out by or on behalf of any of the intelligence services or in the challengeable circumstances described in subsection (7);
- any complaint by a person that he has suffered detriment as a result of any prohibition or restriction in Section 17 on his relying on any civil proceedings (Section 17 imposes various restrictions and prohibitions on the disclosure in court of intercepted material and related information); and
- any other proceedings against any of the intelligence services or people acting on their behalf, or which concern the use of investigatory powers under this Act, any entry on or interference with property, any interference with wireless telegraphy where any of these take place in relation to conduct by any of the public authorities listed in subsection (6). This category only applies to proceedings allocated to the

Tribunal by the Secretary of State. Section 66 makes further provision concerning such orders.

321. *Subsection (6)* limits the Tribunal's jurisdiction in respect of Human Rights Act cases and proceedings allocated to the Tribunal by the Secretary of State. The jurisdiction will only apply to conduct by or on behalf of the police, Customs or intelligence services.

322. *Subsection (7)* qualifies the first and second categories and some elements of the fourth categories of the Tribunal's jurisdiction.

Section 66: Orders allocating proceedings to the Tribunal

323. This Section makes further provision concerning the orders (by affirmative resolution, see Section 78) that the Secretary of State may make to provide for the Tribunal to exercise jurisdiction over certain types of case. It ensures that:

- the Tribunal is given the power to remit proceedings to the court or tribunal which would have had jurisdiction but for the order;
- proceedings before the Tribunal are properly heard and considered;
- information is not disclosed where this might be damaging or prejudicial as described in subsection (2)(b).

Section 67: Exercise of the Tribunal's jurisdiction

324. This Section makes further provision concerning the exercise of the Tribunal's jurisdiction under Section 65. It describes how the Tribunal is to hear, consider and investigate complaints and proceedings, confers on the Tribunal the power to award compensation, quash or cancel any warrant or authorisation and require the destruction of records of information.

325. *Subsection (7)* confers powers on the Tribunal. An order to quash or cancel any warrant or authorisation would overturn the decision of the person who authorised such an instrument, and any continued conduct under the terms of the quashed authorisation or examination of information obtained under its authority would not be lawful.

Section 68: Tribunal procedure

326. This Section provides for the Tribunal to determine their own procedure (subject to any rules made by the Secretary of State under Section 69), and requires it to inform certain persons of proceedings, complaints and their determinations, and empowers it to require the cooperation of certain persons in exercising their powers and duties.

327. *Subsection (2)* empowers the Tribunal to require any Commissioner listed in subsection (8) to advise it on any matters falling within his knowledge which are relevant to the Tribunal's functions.

Section 69: Tribunal rules

328. This Section describes those rules which the Secretary of State may make subject to the affirmative resolution procedure to regulate the Tribunal's exercise of its powers, and any matters related to them.

329. *Subsections (2) to (5)* describe rules the Secretary of State may make, without limiting his power to make rules only to those matters listed.

330. *Subsection (6)* requires the Secretary of State, in making any rules, to ensure:

- that proceedings before the Tribunal are properly heard and considered; and
- that information is not disclosed where this might be damaging or prejudicial as described in subsection (2)(b).

331. *Subsection (7)* enables any rules to incorporate, for example, Civil Procedure Rules which have already been made. This avoids the need to create such rules from scratch for the Tribunal where they already exist elsewhere.

332. *Subsections (9) to (11)* provide that where rules governing the conduct of the Tribunal are made for the first time, they be made under a special 40 day procedure. This will ensure that the Tribunal is operational as soon as the substantive provisions in the Act are brought into force. For all subsequent rules, the affirmative resolution procedure will apply.

Section 70: Abolition of jurisdiction in relation to complaints

333. This Section repeals those provisions listed in subsection (2), which provide for the jurisdiction of Tribunals established by other Acts of Parliament to investigate complaints concerning conduct which is in future to be investigated by the Tribunal established in this Act. Those Tribunals may, however, finish their investigation of those cases which they begin to consider before the Act comes into force.

Section 71: Issue and revision of Codes of Practice

334. This Section deals with the issuing of Codes of Practice to explain in greater detail the practical arrangements relating to the use of the provisions of this Act.

335. *Subsections (1) and (2)* require the Secretary of State to issue one or more Codes of Practice covering the powers and duties in this Act and those relating to interference with property or wireless telegraphy in either the Intelligence Services Act 1994 or Part III of the Police Act 1997.

336. *Subsections (3), (4) and (5)* require the Secretary of State to consult on any Codes of Practice, lay the drafts before Parliament and bring them into force through an Order (by affirmative resolution, see Section 78).

Section 72: Effect of Codes of Practice

337. *Subsection (1)* requires any person to take account of any applicable Code of Practice issued under Section 71 while exercising or performing any power or duty under this Act.

338. *Subsection (2)* explains that a failure to comply with a Code of Practice issued under Section 71 will not of itself constitute a criminal offence or civil tort.

339. *Subsection (3)* allows the evidential use of a Code of Practice in court.

340. *Subsection (4)* requires that, where relevant, the statutory bodies described in this subsection must take into account the provisions of a Code of Practice.

Part V: Miscellaneous and Supplemental

Section 73: Conduct in relation to Wireless Telegraphy

341. This section amends Section 5 of the Wireless Telegraphy Act 1949 and is intended to ensure that the interception provisions of that Act comply with the Human Rights Act 1998.

342. *Subsection (1)* transfers the words of the existing section 5 of the Wireless Telegraphy Act to a new subsection 5(1). It also has the effect of removing the general authority to intercept wireless telegraphy which existed for persons acting in their duty as a servant of the Crown, and of changing the authority level which is required to authorise interception of wireless telegraphy from “under the authority of the Secretary of State” to “under the authority of a designated person”.

"Designated person" is defined in the inserted section 5(12)

343. *Subsection (2)* creates new subsections 5(2) to 5(12) to the Wireless Telegraphy Act 1949 as follows:

- 5(2) restricts the ability of a designated person to authorise interception of wireless telegraphy to activity which cannot be warranted or authorised under this Act;
- 5(3) requires that where the an authorisation is granted under the Wireless Telegraphy Act 1949, consideration must be given to both the necessity and proportionality of the interception in the context of what is sought to be achieved through it;
- 5(4) explains the purposes for which an authorisation under the Wireless Telegraphy Act 1949 may be granted;
- 5(5) requires that where a requirement exists to intercept wireless telegraphy which would not meet one of the tests in 5(4) above but would fit within the criteria of this subsection, a separate authority must be sought;
- 5(6) requires a designated person to consider whether that which is sought to be achieved through the interception could be done in another way;
- 5(10) follows on from subsection (2) and explains that where interception of wireless telegraphy is required to be authorised under the Regulation of Investigatory Powers Act, the fact that the applicant cannot be authorised in this way because he is not mentioned as one of the bodies to which the Act applies does not mean that he can rely upon section 5 to obtain authorisation;
- 5(11) explains the meaning of "separate authority".

Section 74: Warrants under the Intelligence Services Act 1994

344. This section changes the test which must be satisfied before a warrant is issued under section 5 of the Intelligence Services Act 1994. Instead of "likely to be of substantial value", the test is now that the Secretary of State must be satisfied that:

- the action is necessary for the purpose of a function of the intelligence agency;
- the action is proportionate to what it seeks to achieve;
- the action authorised by the warrant could not reasonably be achieved by other means.

345. *Subsection (3)* amends the urgent provisions so that a senior official of any department may sign an urgent warrant issued on the oral authority of the Secretary of State. Such a senior official will be a member of the Senior Civil Service or its equivalent in the Diplomatic Service.

Section 75: Authorisations under Part III of the Police Act 1997

346. This Section makes amendments to Part III of the Police Act 1997.

347. *Subsections (2) and (3)* amend section 93 of the Police Act to allow a police authorising officer to authorise interference with property outside his force area solely for the purpose of maintenance or retrieval of equipment. This will allow a chief constable to authorise action to maintain or retrieve a tracking device from a vehicle that has travelled outside the force area, without having to seek authorisation from the chief constable into whose area the vehicle has travelled. In addition it removes the restriction on where a customs officer may act.

348. In the same way that Section 74 amends the Intelligence Services Act 1994, s*ubsections (4) and (5)* introduce the new tests in the Part III authorisation process. These again

require that the action authorised must be necessary and proportionate to what it seeks to achieve and that the action could not reasonably be achieved by other means.

349. *Subsection (5)* provides for an authorising officer of the Royal Ulster Constabulary to authorise interference with property or wireless telegraphy where it is necessary in the interests of national security as well as for the prevention or detection of serious crime. This is required because of the particular responsibilities of the Chief Constable of the RUC in relation to counter-terrorism.

350. *Subsections (6), (7) and (8)* extend the provisions of Part III to allow the chief constables of the British Transport Police and the Ministry of Defence Police and the Provost Marshals of the three service police forces to be authorising officers and to authorise interference with property or wireless telegraphy within their own jurisdictions. It also allows the Deputy Director General of the National Crime Squad to be an authorising officer in his own right and for the Commissioners of Customs & Excise to designate more than one customs officer to act as an authorising officer.

351. *Subsection (7)* makes an amendment to section 93(6) to provide that "relevant area" for the MOD police means the places described in section 2 of the Ministry of Defence Police Act 1987.

352. *Subsection (8)* makes provision about where the Service Police forces may exercise powers under the 1997 Act.

Section 76: Surveillance operations beginning in Scotland

353. This section provides that surveillance operations which properly begin in Scotland under the Regulation of Investigatory Powers (Scotland) Act can be continued in England under the original authorisation should circumstances arise which make that necessary. But the section stipulates that such authorisations can only be valid for three weeks outside the Scottish jurisdiction.

Section 79: Criminal liability of directors etc

354. This Section provides for personal criminal liability on the part of certain individuals in companies and other bodies corporate.

Section 80: General saving for lawful conduct

355. Section 80 ensures that nothing in this Act makes any actions unlawful unless that is explicitly stated. The availability of an authorisation or a warrant does not mean that it is unlawful not to seek or obtain one. In this respect, the Act must be read with section 6 of the Human Rights Act, which makes it unlawful to act in a way which is incompatible with a Convention right.

Schedule 1: Relevant Public Authorities

356. Part I of Schedule 1 lists those public authorities entitled to use the powers of directed surveillance and covert human intelligence sources under sections 28 and 29 of this Act. Part II of Schedule 1 lists those public authorities entitled to use the power of directed surveillance only, under section 28 of this Act

Schedule 2: Persons Having the Appropriate Permission

357. Schedule 2 deals with the duration and types of appropriate permission which may empower a person to serve a notice under section 49 of this Act requiring disclosure of information. The authority required to grant such permission varies depending on the powers under which unintelligible information is or is likely to be obtained.

Paragraph 1: Requirement that appropriate permission is granted by a judge

358. This paragraph states that subject to the provisions of the paragraphs below, authority to serve a notice must be given by a judge as described in Sub-paragraph (1).

359. The effect of Sub-paragraph (2) is that where a judge's permission has been obtained under this paragraph, no further authority is required to serve a notice.

Paragraph 2: Data obtained under warrant etc

360. This paragraph deals with unintelligible information which is or is likely to be obtained under a statutory power exercised in accordance with:

- a warrant issued by the Secretary of State or a person holding judicial office; or
- an authorisation under Part III of the Police Act 1997.

Examples of legislation under which the Secretary of State may issue a warrant include Chapter I of Part I of this Act and the Intelligence Services Act 1994. Examples of legislation under which a person holding judicial office may issue a warrant include the Police and Criminal Evidence Act 1984 and the Drug Trafficking Act 1994.

361. *Sub-paragraph (2)* states that the warrant or authorisation may empower a person to serve a notice requiring disclosure if:

- the warrant or authorisation gave explicit permission for the notice to be given; or
- written permission has been given by the authority since the warrant or authorisation was issued.

362. *Sub-paragraphs (3) to (5)* describe those persons who are capable of having the appropriate permission to serve a notice in relation to material to which this paragraph applies. And *Sub-paragraphs (6) to (8)* describe those persons who may issue a warrant or authorisation in relation to such material.

363. The effect of this paragraph is that where, for example, protected material has been obtained under an interception warrant, the authorisation to serve a disclosure notice may be granted by the Secretary of State.

364. *Sub-paragraph (9)* excludes from this paragraph unintelligible information:

- which has been obtained under a statutory power without a warrant; but
- which has been obtained in the course of, or in connection with, an exercise of another power for which a warrant was required.

365. This might include, for example, cases where a constable has a right to enter premises under a warrant and while on the premises uncovers matter which he suspects to be evidence of a crime unrelated to the warrant itself, in accordance with e.g. section 19 of the Police and Criminal Evidence Act 1984 (PACE).

Paragraph 3: Data obtained by the intelligence services under statute but without a warrant

366. This paragraph deals with unintelligible information which is, or is likely to be, lawfully obtained by the intelligence services but not under a warrant issued by the Secretary of State. This might include, for example, material obtained under a directed surveillance authorisation given under Part II of this Act.

367. *Sub-paragraph (2)* enables the Secretary of State to give authority for a notice to be served in such instances.

Paragraph 4: Data obtained under statute by other persons but without a warrant

368. This paragraph deals with unintelligible information which is or is likely to be obtained by certain agencies (other than the intelligence services) under statutory powers but not under a warrant issued by the Secretary of State or judicial authority. This includes, for example, material obtained by the police under powers conferred by section 19 of PACE.

369. The effect of Sub-paragraph (2) is that senior officers of the police, customs and excise and armed forces (as described in Paragraph 6) may authorise the service of a written notice in relation to material to which this paragraph applies.

370. The effect of sub-paragraph (3) is that where material to which this paragraph applies is obtained by agencies other than those described in Sub-paragraph (2), authority to serve a written notice is to be given by a judge, provided that the stipulations set out in Sub-paragraph (4) are complied with.

Paragraph 5: Data obtained without the exercise of statutory powers

371. This paragraph deals with unintelligible information which is or is likely to come into the possession of an intelligence service, the police or customs and excise by any other lawful means not involving the exercise of statutory powers (e.g. material which has been voluntarily handed over).

372. The effect of Sub-paragraph (2) is to enable the Secretary of State to give his permission to serve a notice in relation to material, obtained by an intelligence service, falling under this paragraph.

Paragraph 6: General requirements relating to the appropriate permission

373. This paragraph makes some further stipulations about the categories of person who may be empowered to require disclosure. It also makes some stipulations about the permissions that may be given by members of the police, customs and excise and the armed forces.

374. *Sub-paragraph (3)* states that in the case of information which has come into the police's possession by means of powers to stop and search vehicles and pedestrians under the Terrorism Act 2000 or the Prevention of Terrorism (Temporary Provisions) Act 1989 (PTA), those able to authorise the serving of notice must be an officer of police of or above the rank specified in section 44 and section 13A of those Acts respectively.

Section 13A of the PTA, for example, specifies such ranks as:

- *commander of the metropolitan police, as respects the metropolitan police area;*
- *commander of the City of London police, as respects the City of London; or*
- *assistant chief constable for any other police area.*

Paragraph 7: Duration of permission

375. This paragraph provides for the duration of the validity of authorisations to serve a notice and prevents the issue of a notice after the authorisation has expired.

Paragraph 8: Formalities for permissions granted by the Secretary of State

376. This paragraph states that any permissions granted by the Secretary of State in accordance with Schedule 2 may only be granted:

- if signed by him personally; or
- if signed by a member of the Senior Civil Service (or Diplomatic Service equivalent) and expressly authorised by the Secretary of State. The express

authorisation must be in relation to that particular warrant (i.e. there can be no standing authorisation).

Schedule 3: The Tribunal

377. This Schedule provides for the constitution of the Tribunal established under Section 65.

Paragraph 1: Membership of the Tribunal

378. This paragraph determines the membership of the Tribunal.

379. *Sub-paragraph (1)* ensures that members of the Tribunal may be drawn from the legal profession in all parts of the United Kingdom.

> *"High Judicial Office" is defined in Section 25 of the Appellate Jurisdiction Act 1876 as follows:*
>
> *"'High Judicial Office' means any of the following offices; that is to say*
>
> *The office of Lord Chancellor of Great Britain… or of Judge of one of Her Majesty's superior courts of Great Britain and Ireland:*
>
> *'Superior courts of Great Britain and Ireland' means and includes*
>
> *As to England, Her Majesty's High Court of Justice and Her Majesty's Court of Appeal; and*
>
> *As to Northern Ireland, Her Majesty's High Court of Justice in Northern Ireland and Her Majesty's Court of Appeal in Northern Ireland; and*
>
> *As to Scotland, the Court of Session."*
>
> *The Appellate Jurisdiction Act of 1887 amended the term 'High Judicial Office' in Section 5 to include the office of a Lord of Appeal in Ordinary and the office of a member of the Judicial Committee of the Privy Council.*
>
> *The requirement of ten years' standing means that only those eligible for appointment to the judiciary can serve.*
>
> *The Courts and Legal Services Act 1990 states that a person has a "general qualification" if he has a right of audience in relation to any class of proceedings in any part of the Supreme Court, or all proceedings in county courts or magistrates' courts.*

380. Sub-paragraph (3) limits the term of office to five years. A member whose term of office expires is eligible for reappointment. Were he to serve a second time he would have to be re-appointed by further Letters Patent. There is no retirement age.

381. Sub-paragraph (4) provides the means whereby a member may resign.

Paragraph 2: President and Vice-President

382. This paragraph establishes the positions of President and Vice-President who will be members of the Tribunal.

Paragraph 3: Members of the Tribunal with special responsibilities

383. This paragraph requires the President of the Tribunal:

- to give one or more members of the Tribunal special responsibility for matters involving the intelligence services; and
- to ensure that in the consideration or hearing of any complaints or proceedings considered by the Tribunal which relate to an allegation against any of the

intelligence services or their members or to conduct by or on behalf of any of those services or their members, the Tribunal on that occasion includes one or more of the members with such special responsibility.

Paragraph 4: Salaries and expenses

384. This paragraph deals with the payments of the members of the Tribunal and of its expenses.

Paragraph 5: Officers

385. *Sub-paragraph (1)* provides for the appointment of officers of the Tribunal by the Secretary of State, after consultation with the Tribunal. The Secretary of State may not therefore proceed unilaterally to make appointments. The provision itself places no limitation on the number of officers and (subject to Treasury approval as numbers) allows flexibility over the numbers, grades and individuals.

386. *Sub-paragraph (2)* enables an officer who is so authorised by the Tribunal to obtain documents or information on the Tribunal's behalf.

Paragraph 6: Parliamentary disqualification

387. The parts of the Schedules referred to in this paragraph list the bodies whose members are disqualified from membership of the House of Commons and the Northern Ireland Assembly respectively. They include Tribunals and public Boards, Commissions and Councils. Members of this Tribunal (as people paid for adjudicating in a quasi-judicial capacity on the decisions of Ministers, and able to overturn those decisions) clearly fall within the category of those who are normally disqualified.

Schedule 4

Paragraph 8: The Police Act 1997 (c.50)

388. This makes necessary consequential changes in the light of the amendments to Part III of the Police Act 1997. These take account of the extension of authorising powers to the Ministry of Defence Police, the British Transport Police, the Service Police, the three service police forces, the Deputy Director General of the National Crime Squad and additional designated customs officers.

389. *Sub-paragraph (10*) extends the functions of the Chief Surveillance Commissioner so that he reports annually to the Prime Minister and at any other time on any matters arising from his functions in relation to Part III of the Police Act 1997 or Part II of this Act.

390. *Sub-paragraph (11)* imposes a duty on those exercising functions under these provisions to disclose or provide the Chief Surveillance Commissioner with any documents or information he requires to enable him to carry out his functions. It also imposes a duty on every Commissioner to give the Tribunal established under section 65 of this Act all such assistance as may be required.

COMMENCEMENT DATE

391. Section 83(2) provides that the provisions of this Act will come into force as set out by the Secretary of State by order.

Hansard References

The following table sets out the dates and hansard references for each stage of this Act's passage through Parliament.

Stage	***Date***	***Hansard Reference***
House Of Commons		
Introduction	9 February 2000	Col 251 – 252
Second Reading	6 March 2000	Col 767-838
Committee	1st Sitting, 14 March 2000	Standing Committee F
	2nd Sitting, 16 March 2000	
	3rd Sitting, 16 March 2000	
	4th Sitting, 21 March 2000	
	5th Sitting, 23 March 2000	
	6th Sitting, 28 March 2000	
	7th Sitting, 28 March 2000	
	8th Sitting, 30 March 2000	
	9th Sitting, 4 April 2000	
	10th Sitting, 4 April 2000	
	11th Sitting, 6 April 2000	
Report and Third Reading	8 May 2000	Col 531 – 618
House of Lords		
Introduction	9 May 2000	Col 1373
Second Reading	25 May 2000	Col 880 – 913
Committee	12 June 2000	Col 1404 – 1508
19 June 2000	Col 11 – 146	
28 June 2000	Col 900 -1058	
Report	12 July 2000	Col 255 –364
Third Reading	19 July 2000	Col 1017 - 1081

Royal Assent – 28 July 2000	House of Lords Hansard volume Col.
	House of Commons Hansard volume Col.