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

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.