Investigatory Powers Act 2016

2016 CHAPTER 25

PART 1

GENERAL PRIVACY PROTECTIONS

Overview and general privacy duties

1 Overview of Act

(1) This Act sets out the extent to which certain investigatory powers may be used to interfere with privacy.

(2) This Part imposes certain duties in relation to privacy and contains other protections for privacy.

(3) These other protections include offences and penalties in relation to—

(a) the unlawful interception of communications, and

(b) the unlawful obtaining of communications data.

(4) This Part also abolishes and restricts various general powers to obtain communications data and restricts the circumstances in which equipment interference, and certain requests about the interception of communications, can take place.

(5) Further protections for privacy—

(a) can be found, in particular, in the regimes provided for by Parts 2 to 7 and in the oversight arrangements in Part 8, and

(b) also exist—

(i) by virtue of the Human Rights Act 1998,

(ii) in section 55 of the Data Protection Act 1998 (unlawful obtaining etc. of personal data),

(iii) in section 48 of the Wireless Telegraphy Act 2006 (offence of interception or disclosure of messages),

(iv) in sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences),

(v) in the common law offence of misconduct in public office, and

(vi) elsewhere in the law.

(6) The regimes provided for by Parts 2 to 7 are as follows—

(a) Part 2 and Chapter 1 of Part 6 set out circumstances (including under a warrant) in which the interception of communications is lawful and make further provision about the interception of communications and the treatment of material obtained in connection with it,

(b) Part 3 and Chapter 2 of Part 6 set out circumstances in which the obtaining of communications data is lawful in pursuance of an authorisation or under a warrant and make further provision about the obtaining and treatment of such data,

(c) Part 4 makes provision for the retention of certain communications data in pursuance of a notice,

(d) Part 5 and Chapter 3 of Part 6 deal with equipment interference warrants, and

(e) Part 7 deals with bulk personal dataset warrants.

(7) As to the rest of the Act—

(a) Part 8 deals with oversight arrangements for regimes in this Act and elsewhere, and

(b) Part 9 contains miscellaneous and general provisions including amendments to sections 3 and 5 of the Intelligence Services Act 1994 and provisions about national security and combined warrants and authorisations.

2 General duties in relation to privacy

(1) Subsection (2) applies where a public authority is deciding whether—

(a) to issue, renew or cancel a warrant under Part 2, 5, 6 or 7,

(b) to modify such a warrant,

(c) to approve a decision to issue, renew or modify such a warrant,

(d) to grant, approve or cancel an authorisation under Part 3,

(e) to give a notice in pursuance of such an authorisation or under Part 4 or section 252, 253 or 257,

(f) to vary or revoke such a notice,

(g) to approve a decision to give or vary a notice under Part 4 or section 252, 253 or 257,

(h) to approve the use of criteria under section 153, 194 or 222,

(i) to give an authorisation under section 219(3)(b),

(j) to approve a decision to give such an authorisation, or

(k) to apply for or otherwise seek any issue, grant, giving, modification, variation or renewal of a kind falling within paragraph (a), (b), (d), (e), (f) or (i).

(2) The public authority must have regard to—

(a) whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means,

(b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information,

(c) the public interest in the integrity and security of telecommunication systems and postal services, and

(d) any other aspects of the public interest in the protection of privacy.

(3) The duties under subsection (2)—

(a) apply so far as they are relevant in the particular context, and

(b) are subject to the need to have regard to other considerations that are also relevant in that context.

(4) The other considerations may, in particular, include—

(a) the interests of national security or of the economic well-being of the United Kingdom,

(b) the public interest in preventing or detecting serious crime,

(c) other considerations which are relevant to—

(i) whether the conduct authorised or required by the warrant, authorisation or notice is proportionate, or

(ii) whether it is necessary to act for a purpose provided for by this Act,

(d) the requirements of the Human Rights Act 1998, and

(e) other requirements of public law.

(5) For the purposes of subsection (2)(b), examples of sensitive information include—

(a) items subject to legal privilege,

(b) any information identifying or confirming a source of journalistic information, and

(c) relevant confidential information within the meaning given by paragraph 2(4) of Schedule 7 (certain information held in confidence and consisting of personal records, journalistic material or communications between Members of Parliament and their constituents).

(6) In this section "public authority" includes the relevant judicial authority (within the meaning of section 75) where the relevant judicial authority is deciding whether to approve under that section an authorisation under Part 3.

Prohibitions against unlawful interception

3 Offence of unlawful interception

(1) A person commits an offence if—

(a) the person intentionally intercepts a communication in the course of its transmission by means of—

(i) a public telecommunication system,

(ii) a private telecommunication system, or

(iii) a public postal service,

(b) the interception is carried out in the United Kingdom, and

(c) the person does not have lawful authority to carry out the interception.

(2) But it is not an offence under subsection (1) for a person to intercept a communication in the course of its transmission by means of a private telecommunication system if the person—

(a) is a person with a right to control the operation or use of the system, or

(b) has the express or implied consent of such a person to carry out the interception.

(3) Sections 4 and 5 contain provision about—

(a) the meaning of "interception", and

(b) when interception is to be regarded as carried out in the United Kingdom.

(4) Section 6 contains provision about when a person has lawful authority to carry out an interception.

(5) For the meaning of the terms used in subsection (1)(a)(i) to (iii), see sections 261 and 262.

(6) A person who is guilty of an offence under subsection (1) is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;

(c) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(7) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

4 Definition of "interception" etc.

Interception in relation to telecommunication systems

(1) For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if—

(a) the person does a relevant act in relation to the system, and

(b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.

For the meaning of "content" in relation to a communication, see section 261(6).

(2) In this section "relevant act", in relation to a telecommunication system, means—

(a) modifying, or interfering with, the system or its operation;

(b) monitoring transmissions made by means of the system;

(c) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.

(3) For the purposes of this section references to modifying a telecommunication system include references to attaching any apparatus to, or otherwise modifying or interfering with—

(a) any part of the system, or

(b) any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system.

(4) In this section "relevant time", in relation to a communication transmitted by means of a telecommunication system, means—

(a) any time while the communication is being transmitted, and

(b) any time when the communication is stored in or by the system (whether before or after its transmission).

(5) For the purposes of this section, the cases in which any content of a communication is to be taken to be made available to a person at a relevant time include any case in which any of the communication is diverted or recorded at a relevant time so as to make any content of the communication available to a person after that time.

(6) In this section "wireless telegraphy" and "wireless telegraphy apparatus" have the same meaning as in the Wireless Telegraphy Act 2006 (see sections 116 and 117 of that Act).

Interception in relation to postal services

(7) Section 125(3) of the Postal Services Act 2000 applies for the purposes of determining for the purposes of this Act whether a postal item is in the course of its transmission by means of a postal service as it applies for the purposes of determining for the purposes of that Act whether a postal packet is in course of transmission by post.

Interception carried out in the United Kingdom

(8) For the purposes of this Act the interception of a communication is carried out in the United Kingdom if, and only if—

(a) the relevant act or, in the case of a postal item, the interception is carried out by conduct within the United Kingdom, and

(b) the communication is intercepted—

(i) in the course of its transmission by means of a public telecommunication system or a public postal service, or

(ii) in the course of its transmission by means of a private telecommunication system in a case where the sender or intended recipient of the communication is in the United Kingdom.

5 Conduct that is not interception

(1) References in this Act to the interception of a communication do not include references to the interception of any communication broadcast for general reception.

(2) References in this Act to the interception of a communication in the course of its transmission by means of a postal service do not include references to—

(a) any conduct that takes place in relation only to so much of the communication as consists of any postal data comprised in, included as part of, attached to, or logically associated with a communication (whether by the sender or otherwise) for the purposes of any postal service by means of which it is being or may be transmitted, or

(b) any conduct, in connection with conduct falling within paragraph (a), that gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purpose of identifying such postal data.

For the meaning of "postal data", see section 262.

6 Definition of "lawful authority"

(1) For the purposes of this Act, a person has lawful authority to carry out an interception if, and only if—

(a) the interception is carried out in accordance with—

(i) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2, or

(ii) a bulk interception warrant under Chapter 1 of Part 6,

(b) the interception is authorised by any of sections 44 to 52, or

(c) in the case of a communication stored in or by a telecommunication system, the interception—

(i) is carried out in accordance with a targeted equipment interference warrant under Part 5 or a bulk equipment interference warrant under Chapter 3 of Part 6,

(ii) is in the exercise of any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property, or

(iii) is carried out in accordance with a court order made for that purpose.

(2) Conduct which has lawful authority for the purposes of this Act by virtue of subsection (1)(a) or (b) is to be treated as lawful for all other purposes.

(3) Any other conduct which—

(a) is carried out in accordance with a warrant under Chapter 1 of Part 2 or a bulk interception warrant, or

(b) is authorised by any of sections 44 to 52,

is to be treated as lawful for all purposes.

7 Monetary penalties for certain unlawful interceptions

(1) The Investigatory Powers Commissioner may serve a monetary penalty notice on a person if conditions A and B are met.

(2) A monetary penalty notice is a notice requiring the person on whom it is served to pay to the Investigatory Powers Commissioner ("the Commissioner") a monetary penalty of an amount determined by the Commissioner and specified in the notice.

(3) Condition A is that the Commissioner considers that—

(a) the person has intercepted, in the United Kingdom, any communication in the course of its transmission by means of a public telecommunication system,

(b) the person did not have lawful authority to carry out the interception, and

(c) the person was not, at the time of the interception, making an attempt to act in accordance with an interception warrant which might, in the opinion of the Commissioner, explain the interception.

(4) Condition B is that the Commissioner does not consider that the person has committed an offence under section 3(1).

(5) The amount of a monetary penalty determined by the Commissioner under this section must not exceed £50,000.

(6) Schedule 1 (which makes further provision about monetary penalty notices) has effect.

(7) In this section "interception warrant" means—

(a) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2, or

(b) a bulk interception warrant under Chapter 1 of Part 6.

(8) For the meaning of "interception" and other key expressions used in this section, see sections 4 to 6.

8 Civil liability for certain unlawful interceptions

(1) An interception of a communication is actionable at the suit or instance of—

(a) the sender of the communication, or

(b) the recipient, or intended recipient, of the communication,

if conditions A to D are met.

(2) Condition A is that the interception is carried out in the United Kingdom.

(3) Condition B is that the communication is intercepted—

(a) in the course of its transmission by means of a private telecommunication system, or

(b) in the course of its transmission, by means of a public telecommunication system, to or from apparatus that is part of a private telecommunication system.

(4) Condition C is that the interception is carried out by, or with the express or implied consent of, a person who has the right to control the operation or use of the private telecommunication system.

(5) Condition D is that the interception is carried out without lawful authority.

(6) For the meaning of "interception" and other key expressions used in this section, see sections 4 to 6.

9 Restriction on requesting interception by overseas authorities

(1) This section applies to a request for any authorities of a country or territory outside the United Kingdom to carry out the interception of communications sent by, or intended for, an individual who the person making the request believes will be in the British Islands at the time of the interception.

(2) A request to which this section applies may not be made by or on behalf of a person in the United Kingdom unless—

(a) a targeted interception warrant has been issued under Chapter 1 of Part 2 authorising the person to whom it is addressed to secure the interception of communications sent by, or intended for, that individual, or

(b) a targeted examination warrant has been issued under that Chapter authorising the person to whom it is addressed to carry out the selection of the content of such communications for examination.

10 Restriction on requesting assistance under mutual assistance agreements etc.

(1) This section applies to—

(a) a request for assistance under an EU mutual assistance instrument, and

(b) a request for assistance in accordance with an international mutual assistance agreement.

(2) A request to which this section applies may not be made by or on behalf of a person in the United Kingdom to the competent authorities of a country or territory outside the United Kingdom unless a mutual assistance warrant has been issued under Chapter 1 of Part 2 authorising the making of the request.

(3) In this section—

"EU mutual assistance instrument" means an EU instrument which—

(a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,

(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and

(c) is designated as an EU mutual assistance instrument by regulations made by the Secretary of State;

"international mutual assistance agreement" means an international agreement which—

(a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,

(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and

(c) is designated as an international mutual assistance agreement by regulations made by the Secretary of State.

Prohibition against unlawful obtaining of communications data

11 Offence of unlawfully obtaining communications data

(1) A relevant person who, without lawful authority, knowingly or recklessly obtains communications data from a telecommunications operator or a postal operator is guilty of an offence.

(2) In this section "relevant person" means a person who holds an office, rank or position with a relevant public authority (within the meaning of Part 3).

(3) Subsection (1) does not apply to a relevant person who shows that the person acted in the reasonable belief that the person had lawful authority to obtain the communications data.

(4) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

Abolition or restriction of powers to obtain communications data

12 Abolition or restriction of certain powers to obtain communications data

(1) Schedule 2 (which repeals certain information powers so far as they enable public authorities to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator) has effect.

(2) Any general information power which—

(a) would (apart from this subsection) enable a public authority to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator, and

(b) does not involve a court order or other judicial authorisation or warrant and is not a regulatory power or a relevant postal power,

is to be read as not enabling the public authority to secure such a disclosure.

(3) A regulatory power or relevant postal power which enables a public authority to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator may only be exercised by the public authority for that purpose if it is not possible for the authority to use a power under this Act to secure the disclosure of the data.

(4) The Secretary of State may by regulations modify any enactment in consequence of subsection (2).

(5) In this section "general information power" means—

(a) in relation to disclosure by a telecommunications operator, any power to obtain information or documents (however expressed) which—

(i) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and

(ii) does not deal (whether alone or with other matters) specifically with telecommunications operators or any class of telecommunications operators, and

(b) in relation to disclosure by a postal operator, any power to obtain information or documents (however expressed) which—

(i) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and

(ii) does not deal (whether alone or with other matters) specifically with postal operators or any class of postal operators.

(6) In this section—

"power" includes part of a power,

"regulatory power" means any power to obtain information or documents (however expressed) which—

(a) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and

(b) is exercisable in connection with the regulation of—

(i) telecommunications operators, telecommunications services or telecommunication systems, or

(ii) postal operators or postal services,

"relevant postal power" means any power to obtain information or documents (however expressed) which—

(a) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and

(b) is exercisable in connection with the conveyance or expected conveyance of any postal item into or out of the United Kingdom,

and references to powers include duties (and references to enabling and exercising are to be read as including references to requiring and performing).

Restrictions on interference with equipment

13 Mandatory use of equipment interference warrants

(1) An intelligence service may not, for the purpose of obtaining communications, private information or equipment data, engage in conduct which could be authorised by an equipment interference warrant except under the authority of such a warrant if—

(a) the intelligence service considers that the conduct would (unless done under lawful authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences), and

(b) there is a British Islands connection.

(2) For the purpose of this section, there is a British Islands connection if—

(a) any of the conduct would take place in the British Islands (regardless of the location of the equipment which would, or may, be interfered with),

(b) the intelligence service believes that any of the equipment which would, or may, be interfered with would, or may, be in the British Islands at some time while the interference is taking place, or

(c) a purpose of the interference is to obtain—

(i) communications sent by, or to, a person who is, or whom the intelligence service believes to be, for the time being in the British Islands,

(ii) private information relating to an individual who is, or whom the intelligence service believes to be, for the time being in the British Islands, or

(iii) equipment data which forms part of, or is connected with, communications or private information falling within sub-paragraph (i) or (ii).

(3) This section does not restrict the ability of the head of an intelligence service to apply for an equipment interference warrant in cases where—

(a) the intelligence service does not consider that the conduct for which it is seeking authorisation would (unless done under lawful authority) constitute

one or more offences under sections 1 to 3A of the Computer Misuse Act 1990, or

(b) there is no British Islands connection.

(4) In this section—

"communications", "private information" and "equipment data" have the same meaning as in Part 5 (see section 135);

"equipment interference warrant" means—

(a) a targeted equipment interference warrant under Part 5;

(b) a bulk equipment interference warrant under Chapter 3 of Part 6.

14 Restriction on use of section 93 of the Police Act 1997

(1) A person may not, for the purpose of obtaining communications, private information or equipment data, make an application under section 93 of the Police Act 1997 for authorisation to engage in conduct which could be authorised by a targeted equipment interference warrant under Part 5 if the applicant considers that the conduct would (unless done under lawful authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences).

(2) In this section, "communications", "private information" and "equipment data" have the same meaning as in Part 5 (see section 135).

PART 2

LAWFUL INTERCEPTION OF COMMUNICATIONS

CHAPTER 1

INTERCEPTION AND EXAMINATION WITH A WARRANT

Warrants under this Chapter

15 Warrants that may be issued under this Chapter

(1) There are three kinds of warrant that may be issued under this Chapter—

(a) targeted interception warrants (see subsection (2)),

(b) targeted examination warrants (see subsection (3)), and

(c) mutual assistance warrants (see subsection (4)).

(2) A targeted interception warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following—

(a) the interception, in the course of their transmission by means of a postal service or telecommunication system, of communications described in the warrant;

(b) the obtaining of secondary data from communications transmitted by means of a postal service or telecommunication system and described in the warrant (see section 16);

(c) the disclosure, in any manner described in the warrant, of anything obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(3) A targeted examination warrant is a warrant which authorises the person to whom it is addressed to carry out the selection of relevant content for examination, in breach of the prohibition in section 152(4) (prohibition on seeking to identify communications of individuals in the British Islands).

In this Part "relevant content", in relation to a targeted examination warrant, means any content of communications intercepted by an interception authorised or required by a bulk interception warrant under Chapter 1 of Part 6.

(4) A mutual assistance warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following—

(a) the making of a request, in accordance with an EU mutual assistance instrument or an international mutual assistance agreement, for the provision of any assistance of a kind described in the warrant in connection with, or in the form of, an interception of communications;

(b) the provision to the competent authorities of a country or territory outside the United Kingdom, in accordance with such an instrument or agreement, of any assistance of a kind described in the warrant in connection with, or in the form of, an interception of communications;

(c) the disclosure, in any manner described in the warrant, of anything obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(5) A targeted interception warrant or mutual assistance warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including—

(i) the interception of communications not described in the warrant, and

(ii) conduct for obtaining secondary data from such communications;

(b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant;

(c) any conduct for obtaining related systems data from any postal operator or telecommunications operator.

(6) For the purposes of subsection (5)(c)—

"related systems data", in relation to a warrant, means systems data relating to a relevant communication or to the sender or recipient, or intended recipient, of a relevant communication (whether or not a person), and

"relevant communication", in relation to a warrant, means—

(a) any communication intercepted in accordance with the warrant in the course of its transmission by means of a postal service or telecommunication system, or

(b) any communication from which secondary data is obtained under the warrant.

(7) For provision enabling the combination of targeted interception warrants with certain other warrants or authorisations (including targeted examination warrants), see Schedule 8.

16 Obtaining secondary data

(1) This section has effect for the purposes of this Part.

(2) In relation to a communication transmitted by means of a postal service, references to obtaining secondary data from the communication are references to obtaining such data in the course of the transmission of the communication (as to which, see section 4(7)).

(3) In relation to a communication transmitted by means of a telecommunication system, references to obtaining secondary data from the communication are references to obtaining such data—

(a) while the communication is being transmitted, or

(b) at any time when the communication is stored in or by the system (whether before or after its transmission).

(4) "Secondary data"—

(a) in relation to a communication transmitted by means of a postal service, means any data falling within subsection (5);

(b) in relation to a communication transmitted by means of a telecommunication system, means any data falling within subsection (5) or (6).

(5) The data falling within this subsection is systems data which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise).

(6) The data falling within this subsection is identifying data which—

(a) is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise),

(b) is capable of being logically separated from the remainder of the communication, and

(c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication.

(7) For the meaning of "systems data" and "identifying data", see section 263.

17 Subject-matter of warrants

(1) A warrant under this Chapter may relate to—

(a) a particular person or organisation, or

(b) a single set of premises.

(2) In addition, a targeted interception warrant or targeted examination warrant may relate to—

(a) a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;

(b) more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation;

(c) testing or training activities.

(3) In subsection (2)(c) "testing or training activities" means—

(a) in relation to a targeted interception warrant—

(i) the testing, maintenance or development of apparatus, systems or other capabilities relating to the interception of communications in the course of their transmission by means of a telecommunication system or to the obtaining of secondary data from communications transmitted by means of such a system, or

(ii) the training of persons who carry out, or are likely to carry out, such interception or the obtaining of such data;

(b) in relation to a targeted examination warrant—

(i) the testing, maintenance or development of apparatus, systems or other capabilities relating to the selection of relevant content for examination, or

(ii) the training of persons who carry out, or are likely to carry out, the selection of relevant content for examination.

Power to issue warrants

18 Persons who may apply for issue of a warrant

(1) Each of the following is an "intercepting authority" for the purposes of this Part—

(a) a person who is the head of an intelligence service;

(b) the Director General of the National Crime Agency;

(c) the Commissioner of Police of the Metropolis;

(d) the Chief Constable of the Police Service of Northern Ireland;

(e) the chief constable of the Police Service of Scotland;

(f) the Commissioners for Her Majesty's Revenue and Customs;

(g) the Chief of Defence Intelligence;

(h) a person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.

(2) For the meaning of "head of an intelligence service", see section 263.

(3) An application for the issue of a warrant under this Chapter may only be made on behalf of an intercepting authority by a person holding office under the Crown.

19 Power of Secretary of State to issue warrants

(1) The Secretary of State may, on an application made by or on behalf of an intercepting authority mentioned in section 18(1)(a) to (g), issue a targeted interception warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within section 20,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 53 and 54 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

This is subject to subsection (4).

(2) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within section 20,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that the warrant is or may be necessary to authorise the selection of relevant content for examination in breach of the prohibition in section 152(4) (prohibition on seeking to identify communications of individuals in the British Islands), and

(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

This is subject to subsection (4).

(3) The Secretary of State may, on an application made by or on behalf of an intercepting authority, issue a mutual assistance warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within section 20,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 53 and 54 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

This is subject to subsection (4).

(4) The Secretary of State may not issue a warrant under this section if—

(a) the application is a relevant Scottish application (see section 22), and

(b) in the case of an application for a targeted interception warrant or a targeted examination warrant, the Secretary of State considers that the warrant is necessary only for the purpose of preventing or detecting serious crime.

For the power of the Scottish Ministers to issue warrants under this Chapter, see section 21.

(5) But subsection (4) does not prevent the Secretary of State from doing anything under this section for the purposes specified in section 2(2) of the European Communities Act 1972.

20 Grounds on which warrants may be issued by Secretary of State

(1) This section has effect for the purposes of this Part.

(2) A targeted interception warrant or targeted examination warrant is necessary on grounds falling within this section if it is necessary—

(a) in the interests of national security,

(b) for the purpose of preventing or detecting serious crime, or

(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security (but see subsection (4)).

(3) A mutual assistance warrant is necessary on grounds falling within this section if—

(a) it is necessary for the purpose of giving effect to the provisions of an EU mutual assistance instrument or an international mutual assistance agreement, and

(b) the circumstances appear to the Secretary of State to be equivalent to those in which the Secretary of State would issue a warrant by virtue of subsection (2)(b).

(4) A warrant may be considered necessary as mentioned in subsection (2)(c) only if the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.

(5) A warrant may not be considered necessary on grounds falling within this section if it is considered necessary only for the purpose of gathering evidence for use in any legal proceedings.

(6) The fact that the information which would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on grounds falling within this section.

21 Power of Scottish Ministers to issue warrants

(1) The Scottish Ministers may, on an application made by or on behalf of an intercepting authority mentioned in section 18(1)(a) to (g), issue a targeted interception warrant if—

(a) the application is a relevant Scottish application (see section 22),

(b) the Scottish Ministers consider that the warrant is necessary on grounds falling within subsection (4),

(c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) the Scottish Ministers consider that satisfactory arrangements made for the purposes of sections 53 and 54 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(e) except where the Scottish Ministers consider that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(2) The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—

(a) the application is a relevant Scottish application,

(b) the Scottish Ministers consider that the warrant is necessary on grounds falling within subsection (4),

(c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) the Scottish Ministers consider that the warrant is or may be necessary to authorise the selection of relevant content for examination in breach of the prohibition in section 152(4) (prohibition on seeking to identify communications of individuals in the British Islands), and

(e) except where the Scottish Ministers consider that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(3) The Scottish Ministers may, on an application made by or on behalf of an intercepting authority, issue a mutual assistance warrant if—

(a) the application is a relevant Scottish application,

(b) the Scottish Ministers consider that the warrant is necessary on grounds falling within subsection (4),

(c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) the Scottish Ministers consider that satisfactory arrangements made for the purposes of sections 53 and 54 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(e) except where the Scottish Ministers consider that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(4) A warrant is necessary on grounds falling within this subsection if—

(a) in the case of a targeted interception warrant or targeted examination warrant, it is necessary for the purposes of preventing or detecting serious crime, and

(b) in the case of a mutual assistance warrant—

(i) it is necessary for the purpose of giving effect to the provisions of an EU mutual assistance instrument or an international mutual assistance agreement, and

(ii) the circumstances appear to the Scottish Ministers to be equivalent to those in which the Scottish Ministers would issue a warrant by virtue of paragraph (a).

(5) A warrant may not be considered necessary on grounds falling within subsection (4) if it is considered necessary only for the purpose of gathering evidence for use in any legal proceedings.

(6) The fact that the information which would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on grounds falling within subsection (4).

22 "Relevant Scottish applications"

(1) An application for the issue of a warrant under this Chapter is a "relevant Scottish application" for the purposes of this Chapter if any of conditions A to C is met.

In this section "the applicant" means the person by whom, or on whose behalf, the application is made.

(2) Condition A is that—

(a) the application is for the issue of a targeted interception warrant or a targeted examination warrant, and

(b) the warrant, if issued, would relate to—

(i) a person who is in Scotland, or is reasonably believed by the applicant to be in Scotland, at the time of the issue of the warrant, or

(ii) premises which are in Scotland, or are reasonably believed by the applicant to be in Scotland, at that time.

(3) Condition B is that—

(a) the application is for the issue of a mutual assistance warrant which, if issued, would authorise or require—

(i) the making of a request falling within section 15(4)(a), or

(ii) the making of such a request and disclosure falling within section 15(4)(c), and

(b) the application—

(i) is made by, or on behalf of, the chief constable of the Police Service of Scotland, or

(ii) is made by, or on behalf of, the Commissioners for Her Majesty's Revenue and Customs or the Director General of the National Crime Agency for the purpose of preventing or detecting serious crime in Scotland.

(4) Condition C is that—

(a) the application is for the issue of a mutual assistance warrant which, if issued, would authorise or require—

(i) the provision of assistance falling within section 15(4)(b), or

(ii) the provision of such assistance and disclosure falling within section 15(4)(c), and

(b) the warrant, if issued, would relate to—

(i) a person who is in Scotland, or is reasonably believed by the applicant to be in Scotland, at the time of the issue of the warrant, or

(ii) premises which are in Scotland, or are reasonably believed by the applicant to be in Scotland, at that time.

Approval of warrants by Judicial Commissioners

23 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a person's decision to issue a warrant under this Chapter, a Judicial Commissioner must review the person's conclusions as to the following matters—

(a) whether the warrant is necessary on relevant grounds (see subsection (3)), and

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) In subsection (1)(a) "relevant grounds" means—

(a) in the case of a decision of the Secretary of State to issue a warrant, grounds falling within section 20;

(b) in the case of a decision of the Scottish Ministers to issue a warrant, grounds falling within section 21(4).

(4) Where a Judicial Commissioner refuses to approve a person's decision to issue a warrant under this Chapter, the Judicial Commissioner must give the person written reasons for the refusal.

(5) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a person's decision to issue a warrant under this Chapter, the person may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

24 Approval of warrants issued in urgent cases

(1) This section applies where—

(a) a warrant under this Chapter is issued without the approval of a Judicial Commissioner, and

(b) the person who decided to issue the warrant considered that there was an urgent need to issue it.

(2) The person who decided to issue the warrant must inform a Judicial Commissioner that it has been issued.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to issue the warrant, and

(b) notify the person of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the warrant was issued.

(4) If a Judicial Commissioner refuses to approve the decision to issue a warrant, the warrant—

(a) ceases to have effect (unless already cancelled), and

(b) may not be renewed,

and section 23(5) does not apply in relation to the refusal to approve the decision.

(5) Section 25 contains further provision about what happens if a Judicial Commissioner refuses to approve the decision to issue a warrant.

25 Failure to approve warrant issued in urgent case

(1) This section applies where under section 24(3) a Judicial Commissioner refuses to approve the decision to issue a warrant.

(2) The person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(3) The Judicial Commissioner may—

(a) direct that any of the material obtained under the warrant is destroyed;

(b) impose conditions as to the use or retention of any of that material;

(c) in the case of a targeted examination warrant, impose conditions as to the use of any relevant content selected for examination under the warrant.

(4) The Judicial Commissioner—

(a) may require an affected party to make representations about how the Judicial Commissioner should exercise any function under subsection (3), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(5) Each of the following is an "affected party" for the purposes of subsection (4)—

(a) the person who decided to issue the warrant;

(b) the person to whom the warrant was addressed.

(6) The person who decided to issue the warrant may ask the Investigatory Powers Commissioner to review a decision made by any other Judicial Commissioner under subsection (3).

(7) On a review under subsection (6), the Investigatory Powers Commissioner may—

(a) confirm the Judicial Commissioner's decision, or

(b) make a fresh determination.

(8) Nothing in this section or section 24 affects the lawfulness of—

(a) anything done under the warrant before it ceases to have effect;

(b) if anything is in the process of being done under the warrant when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done which it is not reasonably practicable to stop.

Additional safeguards

26 Members of Parliament etc.

(1) This section applies where—

(a) an application is made to the Secretary of State for the issue of a targeted interception warrant or a targeted examination warrant, and

(b) the purpose of the warrant is—

(i) in the case of a targeted interception warrant, to authorise or require the interception of communications sent by, or intended for, a person who is a member of a relevant legislature, or

(ii) in the case of a targeted examination warrant, to authorise the selection for examination of the content of such communications.

(2) The Secretary of State may not issue the warrant without the approval of the Prime Minister.

(3) In this section "member of a relevant legislature" means—

(a) a member of either House of Parliament;

(b) a member of the Scottish Parliament;

(c) a member of the National Assembly for Wales;

(d) a member of the Northern Ireland Assembly;

(e) a member of the European Parliament elected for the United Kingdom.

27 Items subject to legal privilege

(1) Subsections (2) to (5) apply if—

(a) an application is made by or on behalf of an intercepting authority for a warrant under this Chapter, and

(b) the purpose, or one of the purposes, of the warrant is—

(i) in the case of a targeted interception warrant or mutual assistance warrant, to authorise or require the interception of items subject to legal privilege, or

(ii) in the case of a targeted examination warrant, to authorise the selection of such items for examination.

(2) The application must contain a statement that the purpose, or one of the purposes, of the warrant is to authorise or require the interception, or (in the case of a targeted examination warrant) the selection for examination, of items subject to legal privilege.

(3) In deciding whether to issue the warrant, the person to whom the application is made must have regard to the public interest in the confidentiality of items subject to legal privilege.

(4) The person to whom the application is made may issue the warrant only if the person considers—

(a) that there are exceptional and compelling circumstances that make it necessary to authorise or require the interception, or (in the case of a targeted examination warrant) the selection for examination, of items subject to legal privilege, and

(b) that the arrangements made for the purposes of section 53 or (as the case may be) section 150 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of such items.

(5) But the warrant may not be issued if it is considered necessary only as mentioned in section 20(2)(c).

(6) For the purposes of subsection (4)(a), there cannot be exceptional and compelling circumstances that make it necessary to authorise or require the interception, or the selection for examination, of items subject to legal privilege unless—

(a) the public interest in obtaining the information that would be obtained by the warrant outweighs the public interest in the confidentiality of items subject to legal privilege,

(b) there are no other means by which the information may reasonably be obtained, and

(c) in the case of a warrant considered necessary as mentioned in section 20(2)(b) or (3) or (as the case may be) 21(4), obtaining the information is necessary for the purpose of preventing death or significant injury.

(7) Subsections (8) and (9) apply if—

(a) an application is made by or on behalf of an intercepting authority for a warrant under this Chapter,

(b) the intercepting authority considers that the relevant communications are likely to include items subject to legal privilege, and

(c) subsections (2) to (5) do not apply.

(8) The application must contain—

(a) a statement that the intercepting authority considers that the relevant communications are likely to include items subject to legal privilege, and

(b) an assessment of how likely it is that the relevant communications will include such items.

(9) The person to whom the application is made may issue the warrant only if the person considers that the arrangements made for the purposes of section 53 or (as the case may be) section 150 include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege.

(10) In this section "relevant communications" means—

(a) in relation to a targeted interception warrant or mutual assistance warrant, any communications the interception of which is authorised or required by the warrant;

(b) in relation to a targeted examination warrant, any communications the content of which the warrant authorises to be selected for examination.

(11) Subsections (12) and (13) apply if—

(a) an application is made by or on behalf of an intercepting authority for a warrant under this Chapter,

(b) the purpose, or one of the purposes, of the warrant is—

(i) in the case of a targeted interception warrant or mutual assistance warrant, to authorise or require the interception of communications that, if they were not made with the intention of furthering a criminal purpose, would be items subject to legal privilege, or

(ii) in the case of a targeted examination warrant, to authorise the selection of such communications for examination, and

(c) the intercepting authority considers that the communications ("the targeted communications") are likely to be communications made with the intention of furthering a criminal purpose.

(12) The application must—

(a) contain a statement that the purpose, or one of the purposes, of the warrant is to authorise or require the interception, or (in the case of a targeted examination warrant) the selection for examination, of communications that, if they were not made with the intention of furthering a criminal purpose, would be items subject to legal privilege, and

(b) set out the reasons for believing that the targeted communications are likely to be communications made with the intention of furthering a criminal purpose.

(13) The person to whom the application is made may issue the warrant only if the person considers that the targeted communications are likely to be communications made with the intention of furthering a criminal purpose.

28 Confidential journalistic material

(1) This section applies if—

(a) an application is made by or on behalf of an intercepting authority for a warrant under this Chapter, and

(b) the purpose, or one of the purposes, of the warrant is—

(i) in the case of a targeted interception warrant or mutual assistance warrant, to authorise or require the interception of communications which the intercepting authority believes will be communications containing confidential journalistic material, or

(ii) in the case of a targeted examination warrant, to authorise the selection for examination of journalistic material which the intercepting authority believes is confidential journalistic material.

(2) The application must contain a statement that the purpose, or one of the purposes, of the warrant is—

(a) in the case of a targeted interception warrant or mutual assistance warrant, to authorise or require the interception of communications which the intercepting authority believes will be communications containing confidential journalistic material, or

(b) in the case of a targeted examination warrant, to authorise the selection for examination of journalistic material which the intercepting authority believes is confidential journalistic material.

(3) The person to whom the application is made may issue the warrant only if the person considers that the arrangements made for the purposes of section 53 or (as the case may be) section 150 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of communications containing confidential journalistic material.

(4) For the meaning of "journalistic material" and "confidential journalistic material", see section 264.

29 Sources of journalistic information

(1) This section applies if—

(a) an application is made by or on behalf of an intercepting authority for a warrant under this Chapter, and

(b) the purpose, or one of the purposes, of the warrant is to identify or confirm a source of journalistic information.

(For the meaning of "source of journalistic information", see section 263(1).)

(2) The application must contain a statement that the purpose, or one of the purposes, of the warrant is to identify or confirm a source of journalistic information.

(3) The person to whom the application is made may issue the warrant only if the person considers that the arrangements made for the purposes of section 53 or (as the case may be) section 150 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of communications that identify sources of journalistic information.

Further provision about warrants

30 Decisions to issue warrants to be taken personally by Ministers

(1) The decision to issue a warrant under this Chapter must be taken personally by—

(a) the Secretary of State, or

(b) in the case of a warrant to be issued by the Scottish Ministers, a member of the Scottish Government.

(2) Before a warrant under this Chapter is issued, it must be signed by the person who has taken the decision to issue it.

(3) Subsections (1) and (2) are subject to—

(a) subsection (4), and

(b) section 40 (special rules for certain mutual assistance warrants).

(4) If it is not reasonably practicable for a warrant to be signed by the person who has taken the decision to issue it, the warrant may be signed by a senior official designated by the Secretary of State or (as the case may be) the Scottish Ministers for that purpose.

(5) In such a case, the warrant must contain a statement that—

(a) it is not reasonably practicable for the warrant to be signed by the person who took the decision to issue it, and

(b) the Secretary of State or (as the case may be) a member of the Scottish Government has personally and expressly authorised the issue of the warrant.

(6) In this section "senior official" means—

(a) in the case of a warrant to be issued by the Secretary of State, a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

(b) in the case of a warrant to be issued by the Scottish Ministers, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service.

31 Requirements that must be met by warrants

(1) A warrant under this Chapter must contain a provision stating whether it is a targeted interception warrant, a targeted examination warrant or a mutual assistance warrant.

(2) A warrant issued under this Chapter must be addressed to the person by whom, or on whose behalf, the application for the warrant was made.

(3) A warrant that relates to a particular person or organisation, or to a single set of premises, must name or describe that person or organisation or those premises.

(4) A warrant that relates to a group of persons who share a common purpose or who carry on (or may carry on) a particular activity must—

(a) describe that purpose or activity, and

(b) name or describe as many of those persons as it is reasonably practicable to name or describe.

(5) A warrant that relates to more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation, must—

(a) describe the investigation or operation, and

(b) name or describe as many of those persons or organisations, or as many of those sets of premises, as it is reasonably practicable to name or describe.

(6) A warrant that relates to any testing or training activities must—

(a) describe those activities, and

(b) name or describe as many of the persons within subsection (7) as it is reasonably practicable to name or describe.

"Testing or training activities" has the meaning given by section 17(3).

(7) A person is within this subsection if—

(a) in the case of a targeted interception warrant—

(i) communications from, or intended for, the person will or may be intercepted by an interception authorised or required by the warrant, or

(ii) secondary data will or may be obtained under the warrant from communications from, or intended for, the person;

(b) in the case of a targeted examination warrant, the content of communications from, or intended for, the person may be selected for examination under the warrant.

(8) Where—

(a) a targeted interception warrant or mutual assistance warrant authorises or requires the interception of communications described in the warrant, or the obtaining of secondary data from such communications, or

(b) a targeted examination warrant authorises the selection of the content of communications for examination,

the warrant must specify the addresses, numbers, apparatus, or other factors, or combination of factors, that are to be used for identifying the communications.

(9) Any factor, or combination of factors, specified in accordance with subsection (8) must be one that identifies communications which are likely to be or to include—

(a) communications from, or intended for, any person or organisation named or described in the warrant, or

(b) communications originating on, or intended for transmission to, any premises named or described in the warrant.

(10) In this section any reference to communications from, or intended for, a person or organisation includes communications from, or intended for, anything owned, controlled or operated by that person or organisation.

32 Duration of warrants

(1) A warrant under this Chapter ceases to have effect at the end of the relevant period (see subsection (2)), unless—

(a) it is renewed before the end of that period (see section 33), or

(b) it is cancelled or otherwise ceases to have effect before the end of that period (see sections 24 and 39).

(2) In this section "the relevant period"—

(a) in the case of an urgent warrant which has not been renewed, means the period ending with the fifth working day after the day on which the warrant was issued;

(b) in any other case, means the period of 6 months beginning with—

(i) the day on which the warrant was issued, or

(ii) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) For the purposes of subsection (2)(a) a warrant is an "urgent warrant" if—

(a) the warrant was issued without the approval of a Judicial Commissioner, and

(b) the person who decided to issue the warrant considered that there was an urgent need to issue it.

33 Renewal of warrants

(1) If the renewal conditions are met, a warrant issued under this Chapter may be renewed, at any time during the renewal period, by an instrument issued by the appropriate person (see subsection (3)).

(2) The renewal conditions are—

(a) that the appropriate person considers that the warrant continues to be necessary on any relevant grounds (see subsection (4)),

(b) that the appropriate person considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,

(c) that, in the case of a targeted examination warrant, the appropriate person considers that the warrant continues to be necessary to authorise the selection of relevant content for examination in breach of the prohibition in section 152(4), and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) The appropriate person is—

(a) in the case of a warrant issued by the Secretary of State, the Secretary of State;

(b) in the case of a warrant issued by the Scottish Ministers, a member of the Scottish Government.

(4) "Relevant grounds" means—

(a) in the case of a warrant issued by the Secretary of State, grounds falling within section 20;

(b) in the case of a warrant issued by the Scottish Ministers, grounds falling within section 21(4).

(5) "The renewal period" means—

(a) in the case of an urgent warrant which has not been renewed, the relevant period;

(b) in any other case, the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect.

(6) The decision to renew a warrant must be taken personally by the appropriate person, and the instrument renewing the warrant must be signed by that person.

(7) Section 23 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a warrant as it applies in relation to a decision to issue a warrant (and accordingly any reference in that section to the person who decided to issue the warrant is to be read as a reference to the person who decided to renew it).

(8) Sections 26 to 29 (additional safeguards) apply in relation to a decision to renew a warrant as they apply in relation to a decision to issue a warrant.

(9) In this section—

"the relevant period" has the same meaning as in section 32;

"urgent warrant" is to be read in accordance with subsection (3) of that section.

(10) This section is subject to section 40 (special rules for certain mutual assistance warrants).

34 Modification of warrants

(1) The provisions of a warrant issued under this Chapter may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications that may be made under this section are—

(a) adding, varying or removing the name or description of a person, organisation or set of premises to which the warrant relates, and

(b) adding, varying or removing any factor specified in the warrant in accordance with section 31(8).

(3) But a warrant may not be modified as mentioned in subsection (2)(a) if it relates only to a particular person or organisation, or to a single set of premises, as mentioned in section 17(1).

(4) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

This is subject to section 36(8).

(5) In this Chapter—

(a) a modification adding or varying a name or description as mentioned in paragraph (a) of subsection (2) is referred to as a "major modification", and

(b) any other modification within that subsection is referred to as a "minor modification".

(6) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it.

(7) Sections 35 to 38 contain further provision about making modifications under this section.

35 Persons who may make modifications

(1) A major modification may be made by—

(a) the Secretary of State, in the case of a warrant issued by the Secretary of State,

(b) a member of the Scottish Government, in the case of a warrant issued by the Scottish Ministers, or

(c) a senior official acting on behalf of the Secretary of State or (as the case may be) the Scottish Ministers.

(2) A minor modification may be made by—

(a) the Secretary of State, in the case of a warrant issued by the Secretary of State,

(b) a member of the Scottish Government, in the case of a warrant issued by the Scottish Ministers,

(c) a senior official acting on behalf of the Secretary of State or (as the case may be) the Scottish Ministers,

(d) the person to whom the warrant is addressed, or

(e) a person who holds a senior position in the same public authority as the person mentioned in paragraph (d).

(3) But if a person within subsection (2)(d) or (e) considers that there is an urgent need to make a major modification, that person (as well as a person within subsection (1)) may do so.

Section 38 contains provision about the approval of major modifications made in urgent cases.

(4) Subsections (1) and (3) are subject to section 36(5) and (6) (special rules where any of sections 26 to 29 applies in relation to the making of a major modification).

(5) Subsections (2)(d) and (e) and (3) do not apply in the case of a mutual assistance warrant addressed to a person falling within section 18(1)(h) (competent authorities of overseas countries or territories).

(6) For the purposes of subsection (2)(e) a person holds a senior position in a public authority if—

(a) in the case of any of the intelligence services—

(i) the person is a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service, or

(ii) the person holds a position in the intelligence service of equivalent seniority to such a person;

(b) in the case of the National Crime Agency, the person is a National Crime Agency officer of grade 2 or above;

(c) in the case of the metropolitan police force, the Police Service of Northern Ireland or the Police Service of Scotland, a person is of or above the rank of superintendent;

(d) in the case of Her Majesty's Revenue and Customs, the person is a member of the Senior Civil Service;

(e) in the case of the Ministry of Defence—

(i) the person is a member of the Senior Civil Service, or

(ii) the person is of or above the rank of brigadier, commodore or air commodore.

(7) In this section "senior official" means—

(a) in the case of a warrant issued by the Secretary of State, a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

(b) in the case of a warrant issued by the Scottish Ministers, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service.

36 Further provision about modifications

(1) A person may make a modification within subsection (2) only if the person considers—

(a) that the modification is necessary on any relevant grounds (see subsection (3)), and

(b) that the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct.

(2) The modifications within this subsection are—

(a) a major modification adding the name or description of a person, organisation or set of premises to which the warrant relates, and

(b) a minor modification adding any factor specified in the warrant in accordance with section 31(8).

(3) In subsection (1)(a) "relevant grounds" means—

(a) in the case of a warrant issued by the Secretary of State, grounds falling within section 20;

(b) in the case of a warrant issued by the Scottish Ministers, grounds falling within section 21(4);

and for the purposes of subsection (1) any reference to the Secretary of State in section 20(3)(b) or the Scottish Ministers in section 21(4)(b) is to be read as a reference to the person making the modification.

(4) Sections 26 to 29 (additional safeguards) apply in relation to the making of a major modification within subsection (2)(a) above as they apply in relation to the issuing of a warrant.

(5) Where section 26 applies in relation to the making of a major modification—

(a) the modification must be made by the Secretary of State, and

(b) the modification has effect only if the decision to make the modification has been approved by a Judicial Commissioner.

(6) Where section 27, 28 or 29 applies in relation to the making of a major modification—

(a) the modification must be made by—

(i) the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government, or

(ii) if a senior official acting on behalf of a person within sub-paragraph (i) considers that there is an urgent need to make the modification, that senior official, and

(b) except where the person making the modification considers that there is an urgent need to make it, the modification has effect only if the decision to make the modification has been approved by a Judicial Commissioner.

(7) In a case where any of sections 26 to 29 applies in relation to the making of a major modification, section 23 (approval of warrants by Judicial Commissioners) applies in relation to the decision to make the modification as it applies in relation to a decision to issue a warrant, but as if—

(a) the references in subsection (1)(a) and (b) of that section to the warrant were references to the modification,

(b) any reference to the person who decided to issue the warrant were a reference to the person who decided to make the modification, and

(c) subsection (3) of this section applied for the purposes of subsection (1) of that section as it applies for the purposes of subsection (1) of this section.

Section 38 contains provision about the approval of major modifications made in urgent cases.

(8) If, in a case where any of sections 26 to 29 applies in relation to the making of a major modification, it is not reasonably practicable for the instrument making the modification to be signed by the Secretary of State or (as the case may be) a member of the Scottish Government in accordance with section 34(4), the instrument may be signed by a senior official designated by the Secretary of State or (as the case may be) the Scottish Ministers for that purpose.

(9) In such a case, the instrument making the modification must contain a statement that—

(a) it is not reasonably practicable for the instrument to be signed by the person who took the decision to make the modification, and

(b) the Secretary of State or (as the case may be) a member of the Scottish Government has personally and expressly authorised the making of the modification.

(10) If at any time a person mentioned in section 35(2) considers that any factor specified in a warrant in accordance with section 31(8) is no longer relevant for identifying communications which, in the case of that warrant, are likely to be, or to include, communications falling within section 31(9)(a) or (b), the person must modify the warrant by removing that factor.

(11) In this section "senior official" has the same meaning as in section 35.

37 Notification of major modifications

(1) As soon as is reasonably practicable after a person makes a major modification of a warrant under this Chapter, a Judicial Commissioner must be notified of the modification and the reasons for making it.

(2) But subsection (1) does not apply where—

(a) the modification is made by virtue of section 35(3), or

(b) any of sections 26 to 29 applies in relation to the making of the modification.

(3) Where a major modification is made by a senior official in accordance with section 35(1) or section 36(6)(a)(ii), the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the modification and the reasons for making it.

(4) In this section "senior official" has the same meaning as in section 35.

38 Approval of major modifications made in urgent cases

(1) This section applies where a person makes a major modification of a warrant under this Chapter by virtue of section 35(3).

(2) This section also applies where—

(a) section 27, 28 or 29 applies in relation to the making of a major modification of a warrant under this Chapter,

(b) the person making the modification does so without the approval of a Judicial Commissioner, and

(c) the person considered that there was an urgent need to make the modification.

(3) The person who made the modification must inform the appropriate person that it has been made.

(4) In this section—

"the appropriate person" is—

(a) in a case falling within subsection (1), a designated senior official, and

(b) in a case falling within subsection (2), a Judicial Commissioner,

"designated senior official" means a senior official who has been designated by the Secretary of State or (in the case of warrants issued by the Scottish Ministers) the Scottish Ministers for the purposes of this section, and

"senior official" has the same meaning as in section 35.

(5) The appropriate person must, before the end of the relevant period—

(a) decide whether to approve the decision to make the modification, and

(b) notify the person of the appropriate person's decision.

"The relevant period" means the period ending with the third working day after the day on which the modification was made.

(6) As soon as is reasonably practicable after a designated senior official makes a decision under subsection (5)—

(a) a Judicial Commissioner must be notified of—

(i) the decision, and

(ii) if the senior official has decided to approve the decision to make the modification, the modification in question, and

(b) the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the matters mentioned in paragraph (a)(i) and (ii).

(7) If the appropriate person refuses to approve the decision to make the modification—

(a) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and

(b) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant by virtue of that modification stops as soon as possible,

and, in a case falling within subsection (2) above, section 23(5) does not apply in relation to the refusal to approve the decision.

(8) Nothing in this section affects the lawfulness of—

(a) anything done under the warrant by virtue of the modification before the modification ceases to have effect;

(b) if anything is in the process of being done under the warrant by virtue of the modification when the modification ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done which it is not reasonably practicable to stop.

39 Cancellation of warrants

(1) Any of the appropriate persons may cancel a warrant issued under this Chapter at any time.

(2) If any of the appropriate persons considers that—

(a) a warrant issued under this Chapter is no longer necessary on any relevant grounds, or

(b) the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct,

the person must cancel the warrant.

(3) In subsection (2)(a) "relevant grounds" means—

(a) in the case of a warrant issued by the Secretary of State, grounds falling within section 20;

(b) in the case of a warrant issued by the Scottish Ministers, grounds falling within section 21(4).

(4) For the purpose of this section "the appropriate persons" are—

(a) in the case of a warrant issued by the Secretary of State, the Secretary of State or a senior official acting on behalf of the Secretary of State;

(b) in the case of a warrant issued by the Scottish Ministers, a member of the Scottish Government or a senior official acting on behalf of the Scottish Ministers.

(5) Where a warrant is cancelled under this section, the person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(6) A warrant that has been cancelled under this section may not be renewed.

(7) In this section "senior official" means—

(a) in the case of a warrant issued by the Secretary of State, a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

(b) in the case of a warrant issued by the Scottish Ministers, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service.

(8) See also section 40 (which imposes a duty to cancel mutual assistance warrants in certain circumstances).

40 Special rules for certain mutual assistance warrants

(1) For the purposes of this section a warrant is a "relevant mutual assistance warrant" if—

(a) the warrant is for the purposes of a request for assistance made under an EU mutual assistance instrument or an international mutual assistance agreement by the competent authorities of a country or territory outside the United Kingdom, and

(b) either—

(i) it appears that the interception subject is outside the United Kingdom, or

(ii) the interception authorised or required by the warrant is to take place in relation only to premises outside the United Kingdom.

(2) The decision to issue a relevant mutual assistance warrant may be taken by a senior official designated by the Secretary of State for that purpose.

(3) In such a case, the warrant must contain—

(a) a statement that the warrant is issued for the purposes of a request for assistance made under an EU mutual assistance instrument or an international mutual assistance agreement (as the case may be) by the competent authorities of a country or territory outside the United Kingdom, and

(b) whichever of the following statements is applicable—

(i) a statement that the interception subject appears to be outside the United Kingdom;

(ii) a statement that the interception authorised or required by the warrant is to take place in relation only to premises outside the United Kingdom.

(4) A relevant mutual assistance warrant may be renewed by a senior official designated by the Secretary of State for that purpose; and references in section 33 to the appropriate person include, in the case of such a warrant, references to that senior official.

(5) Where a senior official renews a relevant mutual assistance warrant in accordance with subsection (4), the instrument renewing the warrant must contain—

(a) a statement that the renewal is for the purposes of a request for assistance made under an EU mutual assistance instrument or an international mutual assistance agreement (as the case may be) by the competent authorities of a country or territory outside the United Kingdom, and

(b) whichever of the following statements is applicable—

(i) a statement that the interception subject appears to be outside the United Kingdom;

(ii) a statement that the interception authorised or required by the warrant is to take place in relation only to premises outside the United Kingdom.

(6) Subsection (7) applies in a case where—

(a) a relevant mutual assistance warrant—

(i) was issued containing the statement set out in subsection (3)(b)(i), or

(ii) has been renewed by an instrument containing the statement set out in subsection (5)(b)(i), and

(b) the last renewal (if any) of the warrant was a renewal by a senior official in accordance with subsection (4).

(7) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, believes that the person, group or organisation named or described in the warrant as the interception subject is in the United Kingdom, that person must cancel the warrant under section 39.

(8) In this section—

"the interception subject", in relation to a warrant, means the person, group of persons or organisation to which the warrant relates;

"senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service.

Implementation of warrants

41 Implementation of warrants

(1) This section applies to targeted interception warrants and mutual assistance warrants.

(2) In giving effect to a warrant to which this section applies, the person to whom it is addressed ("the intercepting authority") may (in addition to acting alone) act through, or together with, such other persons as the intercepting authority may require (whether under subsection (3) or otherwise) to provide the authority with assistance in giving effect to the warrant.

(3) For the purpose of requiring any person to provide assistance in relation to a warrant to which this section applies, the intercepting authority may—

(a) serve a copy of the warrant on any person who the intercepting authority considers may be able to provide such assistance, or

(b) make arrangements for the service of a copy of the warrant on any such person.

(4) A copy of a warrant may be served under subsection (3) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(5) For the purposes of this Act, the provision of assistance in giving effect to a warrant to which this section applies includes any disclosure to the intercepting authority, or to persons acting on behalf of the intercepting authority, of anything obtained under the warrant.

(6) References in this section and sections 42 and 43 to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in the warrant.

42 Service of warrants

(1) This section applies to the service of warrants under section 41(3).

(2) A copy of the warrant must be served in such a way as to bring the contents of the warrant to the attention of the person who the intercepting authority considers may be able to provide assistance in relation to it.

(3) A copy of a warrant may be served on a person outside the United Kingdom in any of the following ways (as well as by electronic or other means of service)—

(a) by serving it at the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, at any place in the United Kingdom where the person carries on business or conducts activities;

(b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept service of documents of the same description as a copy of a warrant, by serving it at that address;

(c) by making it available for inspection (whether to the person or to someone acting on the person's behalf) at a place in the United Kingdom (but this is subject to subsection (4)).

(4) A copy of a warrant may be served on a person outside the United Kingdom in the way mentioned in subsection (3)(c) only if—

(a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (3)(a) or (b) or otherwise), and

(b) the intercepting authority takes such steps as the authority considers appropriate for the purpose of bringing the contents of the warrant, and the availability of a copy for inspection, to the attention of the person.

(5) The steps mentioned in subsection (4)(b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.

(6) In this section "the intercepting authority" has the same meaning as in section 41.

43 Duty of operators to assist with implementation

(1) A relevant operator that has been served with a copy of a warrant to which section 41 applies by (or on behalf of) the intercepting authority must take all steps for giving effect to the warrant that are notified to the relevant operator by (or on behalf of) the intercepting authority.

This is subject to subsection (4).

(2) In this section—

"relevant operator" means a postal operator or a telecommunications operator;

"the intercepting authority" has the same meaning as in section 41.

(3) Subsection (1) applies whether or not the relevant operator is in the United Kingdom.

(4) The relevant operator is not required to take any steps which it is not reasonably practicable for the relevant operator to take.

(5) In determining for the purposes of subsection (4) whether it is reasonably practicable for a relevant operator outside the United Kingdom to take any steps in a country or territory outside the United Kingdom for giving effect to a warrant, the matters to be taken into account include the following—

(a) any requirements or restrictions under the law of that country or territory that are relevant to the taking of those steps, and

(b) the extent to which it is reasonably practicable to give effect to the warrant in a way that does not breach any of those requirements or restrictions.

(6) Where obligations have been imposed on a relevant operator ("P") under section 253 (technical capability notices), for the purposes of subsection (4) the steps which it is reasonably practicable for P to take include every step which it would have been reasonably practicable for P to take if P had complied with all of those obligations.

(7) A person who knowingly fails to comply with subsection (1) is guilty of an offence and liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(8) The duty imposed by subsection (1) is enforceable (whether or not the person is in the United Kingdom) by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

CHAPTER 2

OTHER FORMS OF LAWFUL INTERCEPTION

Interception with consent

44 Interception with the consent of the sender or recipient

(1) The interception of a communication is authorised by this section if the sender and the intended recipient of the communication have each consented to its interception.

(2) The interception of a communication is authorised by this section if—

(a) the communication is one sent by, or intended for, a person who has consented to the interception, and

(b) surveillance by means of that interception has been authorised under—

(i) Part 2 of the Regulation of Investigatory Powers Act 2000, or

(ii) the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11).

Interception for administrative or enforcement purposes

45 Interception by providers of postal or telecommunications services

(1) The interception of a communication is authorised by this section if the interception is carried out—

(a) by, or on behalf of, a person who provides a postal service or a telecommunications service, and

(b) for any of the purposes in subsection (2).

(2) The purposes referred to in subsection (1) are—

(a) purposes relating to the provision or operation of the service;

(b) purposes relating to the enforcement, in relation to the service, of any enactment relating to—

(i) the use of postal or telecommunications services, or

(ii) the content of communications transmitted by means of such services;

(c) purposes relating to the provision of services or facilities aimed at preventing or restricting the viewing or publication of the content of communications transmitted by means of postal or telecommunications services.

(3) A reference in this section to anything carried out for purposes relating to the provision or operation of a telecommunications service includes, among other things, a reference to anything done for the purposes of identifying, combating or preventing anything which could affect—

(a) any telecommunication system by means of which the service is provided, or

(b) any apparatus attached to such a system.

46 Interception by businesses etc. for monitoring and record-keeping purposes

(1) Conduct is authorised by this section if it is authorised by regulations made under subsection (2).

(2) The Secretary of State may by regulations authorise conduct of a description specified in the regulations if that conduct appears to the Secretary of State to constitute a legitimate practice reasonably required for the purpose, in connection with the carrying on of any relevant activities (see subsection (4)), of monitoring or keeping a record of—

(a) communications by means of which transactions are entered into in the course of the relevant activities, or

(b) other communications relating to the relevant activities or taking place in the course of the carrying on of those activities.

(3) But nothing in any regulations under subsection (2) may authorise the interception of any communication except in the course of its transmission using apparatus or services provided by or to the person carrying on the relevant activities for use (whether wholly or partly) in connection with those activities.

(4) In this section "relevant activities" means—

(a) any business,

(b) any activities of a government department, the Welsh Government, a Northern Ireland department or any part of the Scottish Administration,

(c) any activities of a public authority, and

(d) any activities of any person or office holder on whom functions are conferred by or under any enactment.

47 Postal services: interception for enforcement purposes

(1) The interception of a communication in the course of its transmission by means of a public postal service is authorised by this section if it is carried out by an officer of Revenue and Customs under section 159 of the Customs and Excise Management Act 1979, as applied by virtue of—

(a) section 105 of the Postal Services Act 2000 (power to open postal items etc.), or

(b) that section and another enactment.

(2) The interception of a communication in the course of its transmission by means of a public postal service is authorised by this section if it is carried out under paragraph 9 of Schedule 7 to the Terrorism Act 2000 (port and border controls).

48 Interception by OFCOM in connection with wireless telegraphy

(1) Conduct falling within subsection (2) is authorised by this section if it is carried out by OFCOM for purposes connected with a relevant matter (see subsection (3)).

(2) The conduct referred to in subsection (1) is—

(a) the interception of a communication in the course of its transmission by means of a telecommunication system;

(b) the obtaining, by or in connection with the interception, of information about the sender or recipient, or intended recipient, of the communication (whether or not a person);

(c) the disclosure of anything obtained by conduct falling within paragraph (a) or (b).

(3) Each of the following is a relevant matter for the purposes of subsection (1)—

(a) the grant of wireless telegraphy licences under the Wireless Telegraphy Act 2006 ("the 2006 Act");

(b) the prevention or detection of anything which constitutes interference with wireless telegraphy;

(c) the enforcement of—

(i) any provision of Part 2 (other than Chapter 2 and sections 27 to 31) or Part 3 of the 2006 Act, or

(ii) any enactment not falling within sub-paragraph (i) that relates to interference with wireless telegraphy.

(4) In this section—

"interference", in relation to wireless telegraphy, has the same meaning as in the Wireless Telegraphy Act 2006 (see section 115(3) of that Act);

"OFCOM" means the Office of Communications established by section 1 of the Office of Communications Act 2002;

"wireless telegraphy" has the same meaning as in the Wireless Telegraphy Act 2006 (see section 116 of that Act).

Interception taking place in certain institutions

49 Interception in prisons

(1) Conduct taking place in a prison is authorised by this section if it is conduct in exercise of any power conferred by or under prison rules.

(2) In this section "prison rules" means any rules made under—

(a) section 47 of the Prison Act 1952,

(b) section 39 of the Prisons (Scotland) Act 1989, or

(c) section 13 of the Prison Act (Northern Ireland) 1953.

(3) In this section "prison" means—

(a) any prison, young offender institution, young offenders centre, secure training centre, secure college or remand centre which—

(i) is under the general superintendence of, or is provided by, the Secretary of State under the Prison Act 1952, or

(ii) is under the general superintendence of, or is provided by, the Department of Justice in Northern Ireland under the Prison Act (Northern Ireland) 1953, or

(b) any prison, young offenders institution or remand centre which is under the general superintendence of the Scottish Ministers under the Prisons (Scotland) Act 1989,

and includes any contracted out prison, within the meaning of Part 4 of the Criminal Justice Act 1991 or section 106(4) of the Criminal Justice and Public Order Act 1994, and any legalised police cells within the meaning of section 14 of the Prisons (Scotland) Act 1989.

50 Interception in psychiatric hospitals etc.

(1) Conduct is authorised by this section if—

(a) it takes place in any hospital premises where high security psychiatric services are provided, and

(b) it is conduct in pursuance of, and in accordance with, any relevant direction given to the body providing those services at those premises.

(2) "Relevant direction" means—

(a) a direction under section 4(3A)(a) of the National Health Service Act 2006, or

(b) a direction under section 19 or 23 of the National Health Service (Wales) Act 2006.

(3) Conduct is authorised by this section if—

(a) it takes place in a state hospital, and

(b) it is conduct in pursuance of, and in accordance with, any direction given to the State Hospitals Board for Scotland under section 2(5) of the National Health Service (Scotland) Act 1978 (regulations and directions as to the exercise of their functions by health boards).

The reference to section 2(5) of that Act is to that provision as applied by Article 5(1) of, and the Schedule to, the State Hospitals Board for Scotland Order 1995 (which applies certain provisions of that Act to the State Hospitals Board).

(4) Conduct is authorised by this section if it is conduct in exercise of any power conferred by or under—

(a) section 281 of the Mental Health (Care and Treatment) (Scotland) Act 2003 (2003 asp 13) (power to withhold correspondence of certain persons detained in hospital), or

(b) section 284 of that Act (powers relating to the use of telephones by certain persons detained in hospital).

(5) In this section—

"high security psychiatric services" has the same meaning as in section 4 of the National Health Service Act 2006;

"hospital premises" has the same meaning as in section 4(3) of that Act;

"state hospital" has the same meaning as in the National Health Service (Scotland) Act 1978.

51 Interception in immigration detention facilities

(1) Conduct taking place in immigration detention facilities is authorised by this section if it is conduct in exercise of any power conferred by or under relevant rules.

(2) In this section—

"immigration detention facilities" means any removal centre, short-term holding facility or pre-departure accommodation;

"removal centre", "short-term holding facility" and "pre-departure accommodation" have the meaning given by section 147 of the Immigration and Asylum Act 1999;

"relevant rules" means—

(a) in the case of a removal centre, rules made under section 153 of that Act;

(b) in the case of a short-term holding facility, rules made under, or having effect by virtue of, section 157 of that Act;

(c) in the case of pre-departure accommodation, rules made under, or having effect by virtue of, section 157A of that Act.

Interception in accordance with overseas requests

52 Interception in accordance with overseas requests

(1) The interception of a communication in the course of its transmission by means of a telecommunication system is authorised by this section if conditions A to D are met.

(2) Condition A is that the interception—

(a) is carried out by or on behalf of a telecommunications operator, and

(b) relates to the use of a telecommunications service provided by the telecommunications operator.

(3) Condition B is that the interception is carried out in response to a request made in accordance with a relevant international agreement by the competent authorities of a country or territory outside the United Kingdom.

In this subsection "relevant international agreement" means an international agreement to which the United Kingdom is a party and which is designated as a relevant international agreement by regulations made by the Secretary of State.

(4) Condition C is that the interception is carried out for the purpose of obtaining information about the communications of an individual—

(a) who is outside the United Kingdom, or

(b) who each of the following persons believes is outside the United Kingdom—

(i) the person making the request;

(ii) the person carrying out the interception.

(5) Condition D is that any further conditions specified in regulations made by the Secretary of State for the purposes of this section are met.

CHAPTER 3

OTHER PROVISIONS ABOUT INTERCEPTION

Restrictions on use or disclosure of material obtained under warrants etc.

53 Safeguards relating to retention and disclosure of material

(1) The issuing authority must ensure, in relation to every targeted interception warrant or mutual assistance warrant issued by that authority, that arrangements are in force for securing that the requirements of subsections (2) and (5) are met in relation to the material obtained under the warrant.

This is subject to subsection (9).

(2) The requirements of this subsection are met in relation to the material obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))—

(a) the number of persons to whom any of the material is disclosed or otherwise made available;

(b) the extent to which any of the material is disclosed or otherwise made available;

(c) the extent to which any of the material is copied;

(d) the number of copies that are made.

(3) For the purposes of this section something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary on any of the grounds falling within section 20 on which a warrant under Chapter 1 of this Part may be necessary,

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the person to whom the warrant is or was addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution, or

(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the material obtained under a warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any relevant grounds for retaining a copy of any material if, and only if—

(a) its retention is not necessary, or not likely to become necessary, on any of the grounds falling within section 20 on which a warrant under Chapter 1 of this Part may be necessary, and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (3) above.

(7) Where—

(a) a communication which has been intercepted in accordance with a targeted interception warrant or mutual assistance warrant is retained, following its examination, for purposes other than the destruction of the communication, and

(b) it is a communication that contains confidential journalistic material or identifies a source of journalistic information,

the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

(8) Subsection (9) applies if—

(a) any material obtained under the warrant has been handed over to any overseas authorities, or

(b) a copy of any such material has been given to any overseas authorities.

(9) To the extent that the requirements of subsections (2) and (5) relate to any of the material mentioned in subsection (8)(a), or to the copy mentioned in subsection (8)(b), the arrangements made for the purposes of this section are not required to secure that those requirements are met (see instead section 54).

(10) In this section—

"copy", in relation to material obtained under a warrant, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the material which identifies the material as having been obtained under the warrant, and

(b) any record which—

(i) refers to any interception or to the obtaining of any material, and

(ii) is a record of the identities of the persons to or by whom the material was sent, or to whom the material relates,

and "copied" is to be read accordingly;

"the issuing authority" means—

(a) the Secretary of State, in the case of warrants issued by the Secretary of State;

(b) the Scottish Ministers, in the case of warrants issued by the Scottish Ministers;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

54 Safeguards relating to disclosure of material overseas

(1) The issuing authority must ensure, in relation to every targeted interception warrant or mutual assistance warrant issued by that authority, that arrangements are in force for securing that—

(a) any material obtained under the warrant is handed over to overseas authorities only if the requirements of subsection (2) are met, and

(b) copies of any such material are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of a warrant if it appears to the issuing authority—

(a) that requirements corresponding to the requirements of section 53(2) and (5) will apply, to such extent (if any) as the issuing authority considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question, and

(b) that restrictions are in force which would prevent, to such extent (if any) as the issuing authority considers appropriate, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in a prohibited disclosure.

(3) In subsection (2)(b) "prohibited disclosure" means a disclosure which, if made in the United Kingdom, would breach the prohibition in section 56(1).

(4) In this section—

"copy" has the same meaning as in section 53;

"the issuing authority" means—

(a) the Secretary of State, in the case of warrants issued by the Secretary of State;

(b) the Scottish Ministers, in the case of warrants issued by the Scottish Ministers;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

55 Additional safeguards for items subject to legal privilege

(1) This section applies where an item subject to legal privilege which has been intercepted in accordance with a targeted interception warrant or mutual assistance warrant is retained, following its examination, for purposes other than the destruction of the item.

(2) The person to whom the warrant is addressed must inform the Investigatory Powers Commissioner of the retention of the item as soon as is reasonably practicable.

(3) Unless the Investigatory Powers Commissioner considers that subsection (5) applies to the item, the Commissioner must—

(a) direct that the item is destroyed, or

(b) impose one or more conditions as to the use or retention of that item.

(4) If the Investigatory Powers Commissioner considers that subsection (5) applies to the item, the Commissioner may nevertheless impose such conditions under subsection (3)(b) as the Commissioner considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege.

(5) This subsection applies to an item subject to legal privilege if—

(a) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and

(b) retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(6) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsection (3), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(7) Each of the following is an "affected party" for the purposes of subsection (6)—

(a) the person who decided to issue the warrant;

(b) the person to whom the warrant is or was addressed.

56 Exclusion of matters from legal proceedings etc.

(1) No evidence may be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings which (in any manner)—

(a) discloses, in circumstances from which its origin in interception-related conduct may be inferred—

(i) any content of an intercepted communication, or

(ii) any secondary data obtained from a communication, or

(b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.

This is subject to Schedule 3 (exceptions).

(2) "Interception-related conduct" means—

(a) conduct by a person within subsection (3) that is, or in the absence of any lawful authority would be, an offence under section 3(1) (offence of unlawful interception);

(b) a breach of the prohibition imposed by section 9 (restriction on requesting interception by overseas authorities);

(c) a breach of the prohibition imposed by section 10 (restriction on requesting assistance under mutual assistance agreements etc.);

(d) the making of an application by any person for a warrant, or the issue of a warrant, under Chapter 1 of this Part;

(e) the imposition of any requirement on any person to provide assistance in giving effect to a targeted interception warrant or mutual assistance warrant.

(3) The persons referred to in subsection (2)(a) are—

(a) any person who is an intercepting authority (see section 18);

(b) any person holding office under the Crown;

(c) any person deemed to be the proper officer of Revenue and Customs by virtue of section 8(2) of the Customs and Excise Management Act 1979;

(d) any person employed by, or for the purposes of, a police force;

(e) any postal operator or telecommunications operator;

(f) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator.

(4) Any reference in subsection (1) to interception-related conduct also includes any conduct taking place before the coming into force of this section and consisting of—

(a) conduct by a person within subsection (3) that—

(i) was an offence under section 1(1) or (2) of the Regulation of Investigatory Powers Act 2000 ("RIPA"), or

(ii) would have been such an offence in the absence of any lawful authority (within the meaning of section 1(5) of RIPA);

(b) conduct by a person within subsection (3) that—

(i) was an offence under section 1 of the Interception of Communications Act 1985, or

(ii) would have been such an offence in the absence of subsections (2) and (3) of that section;

(c) a breach by the Secretary of State of the duty under section 1(4) of RIPA (restriction on requesting assistance under mutual assistance agreements);

(d) the making of an application by any person for a warrant, or the issue of a warrant, under—

(i) Chapter 1 of Part 1 of RIPA, or

(ii) the Interception of Communications Act 1985;

(e) the imposition of any requirement on any person to provide assistance in giving effect to a warrant under Chapter 1 of Part 1 of RIPA.

(5) In this section—

"Inquiries Act proceedings" means proceedings of an inquiry under the Inquiries Act 2005;

"intercepted communication" means any communication intercepted in the course of its transmission by means of a postal service or telecommunication system.

57 Duty not to make unauthorised disclosures

(1) A person to whom this section applies must not make an unauthorised disclosure to another person.

(2) A person makes an unauthorised disclosure for the purposes of this section if—

(a) the person discloses any of the matters within subsection (4) in relation to—

(i) a warrant under Chapter 1 of this Part, or

(ii) a warrant under Chapter 1 of Part 1 of the Regulation of Investigatory Powers Act 2000, and

(b) the disclosure is not an excepted disclosure (see section 58).

(3) This section applies to the following persons—

(a) any person who is an intercepting authority (see section 18);

(b) any person holding office under the Crown;

(c) any person employed by, or for the purposes of, a police force;

(d) any postal operator or telecommunications operator;

(e) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator;

(f) any person to whom any of the matters within subsection (4) have been disclosed in relation to a warrant mentioned in subsection (2)(a).

(4) The matters referred to in subsection (2)(a) are—

(a) the existence or contents of the warrant;

(b) the details of the issue of the warrant or of any renewal or modification of the warrant;

(c) the existence or contents of any requirement to provide assistance in giving effect to the warrant;

(d) the steps taken in pursuance of the warrant or of any such requirement;

(e) any of the material obtained under the warrant.

58 Section 57: meaning of "excepted disclosure"

(1) For the purposes of section 57 a disclosure made in relation to a warrant is an "excepted disclosure" if it falls within any of the Heads set out in—

(a) subsection (2) (disclosures authorised by warrant etc.);

(b) subsection (4) (oversight bodies);

(c) subsection (5) (legal advisers);

(d) subsection (8) (disclosures of a general nature).

(2) Head 1 is—

(a) a disclosure authorised by the warrant;

(b) a disclosure authorised by the person to whom the warrant is or was addressed or under any arrangements made by that person for the purposes of this section;

(c) a disclosure authorised by the terms of any requirement to provide assistance in giving effect to the warrant (including any requirement for disclosure imposed by virtue of section 41(5) or, in the case of a warrant under Chapter 1 of Part 1 of the Regulation of Investigatory Powers Act 2000 ("RIPA"), section 11(9) of RIPA).

(3) But subsection (2)(b) does not apply in the case of a mutual assistance warrant that is or was addressed to a person falling within section 18(1)(h) (competent authorities of overseas countries or territories).

(4) Head 2 is—

(a) in the case of a warrant under Chapter 1 of this Part, a disclosure made to, or authorised by, a Judicial Commissioner;

(b) in the case of a warrant under Chapter 1 of Part 1 of RIPA, a disclosure made to, or authorised by, the Interception of Communications Commissioner or a Judicial Commissioner;

(c) a disclosure made to the Independent Police Complaints Commission for the purposes of facilitating the carrying out of any of its functions;

(d) a disclosure made to the Intelligence and Security Committee of Parliament for the purposes of facilitating the carrying out of any of its functions.

(5) Head 3 is—

(a) a disclosure made by a legal adviser—

(i) in contemplation of, or in connection with, any legal proceedings, and

(ii) for the purposes of those proceedings;

(b) a disclosure made—

(i) by a professional legal adviser ("L") to L's client or a representative of L's client, or

(ii) by L's client, or by a representative of L's client, to L,

in connection with the giving, by L to L's client, of advice about the effect of the relevant provisions (see subsection (7)).

(6) But a disclosure within Head 3 is not an excepted disclosure if it is made with the intention of furthering a criminal purpose.

(7) In subsection (5)(b) "the relevant provisions" means—

(a) in the case of a warrant under Chapter 1 of this Part, the provisions of this Part;

(b) in the case of a warrant under Chapter 1 of Part 1 of RIPA, the provisions of that Chapter.

(8) Head 4 is—

(a) a disclosure that—

(i) is made by a postal operator or a telecommunications operator in accordance with a requirement imposed by regulations made by the Secretary of State, and

(ii) consists of statistical information of a description specified in the regulations;

(b) a disclosure of information that does not relate to any particular warrant under Chapter 1 of this Part or under Chapter 1 of Part 1 of RIPA but relates to any such warrants in general.

(9) Nothing in this section affects the operation of section 56 (which, among other things, prohibits the making of certain disclosures in, for the purposes of or in connection with legal proceedings).

59 Offence of making unauthorised disclosures

(1) A person who fails to comply with section 57(1) commits an offence.

(2) A person who is guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine, or to both.

(3) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure.

Interpretation

60 Part 2: interpretation

(1) In this Part—

"EU mutual assistance instrument" has the meaning given by section 10(3);

"intercepting authority" is to be read in accordance with section 18;

"international mutual assistance agreement" has the meaning given by section 10(3);

"mutual assistance warrant" has the meaning given by section 15(4);

"police force" means any of the following—

(a) any police force maintained under section 2 of the Police Act 1996;

(b) the metropolitan police force;

(c) the City of London police force;

(d) the Police Service of Scotland;

(e) the Police Service of Northern Ireland;

(f) the Ministry of Defence Police;

(g) the Royal Navy Police;

(h) the Royal Military Police;

(i) the Royal Air Force Police;

(j) the British Transport Police Force;

"relevant content", in relation to a targeted examination warrant, has the meaning given by section 15(3);

"relevant Scottish application" has the meaning given by section 22;

"secondary data" has the meaning given by section 16, and references to obtaining secondary data from a communication are to be read in accordance with that section;

"targeted examination warrant" has the meaning given by section 15(3).

(2) In this Part references to a member of a police force, in relation to the Royal Navy Police, the Royal Military Police or the Royal Air Force Police, do not include any member of that force who is not for the time being attached to, or serving with, that force or another of those police forces.

(3) See also—

section 261 (telecommunications definitions),
section 262 (postal definitions),
section 263 (general definitions),
section 264 (general definitions: "journalistic material" etc.),
section 265 (index of defined expressions).

PART 3

AUTHORISATIONS FOR OBTAINING COMMUNICATIONS DATA

Targeted authorisations for obtaining data

61 Power to grant authorisations

(1) Subsection (2) applies if a designated senior officer of a relevant public authority considers—

(a) that it is necessary to obtain communications data for a purpose falling within subsection (7),

(b) that it is necessary to obtain the data—

(i) for the purposes of a specific investigation or a specific operation, or

(ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, and

(c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.

(2) The designated senior officer may authorise any officer of the authority to engage in any conduct which—

(a) is for the purpose of obtaining the data from any person, and

(b) relates to—

(i) a telecommunication system, or

(ii) data derived from a telecommunication system.

(3) Subsections (1) and (2) are subject to—

(a) section 62 (restrictions in relation to internet connection records),

(b) section 63 (additional restrictions on grant of authorisations),

(c) sections 70 and 73 to 75 and Schedule 4 (restrictions relating to certain relevant public authorities),

(d) section 76 (requirement to consult a single point of contact), and

(e) section 77 (Commissioner approval for authorisations to identify or confirm journalistic sources).

(4) Authorised conduct may, in particular, consist of an authorised officer—

(a) obtaining the communications data themselves from any person or telecommunication system,

(b) asking any person whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it), and

(ii) to disclose the data (whether already in the person's possession or subsequently obtained by that person) to a person identified by, or in accordance with, the authorisation, or

(c) requiring by notice a telecommunications operator whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it), and

(ii) to disclose the data (whether already in the operator's possession or subsequently obtained by the operator) to a person identified by, or in accordance with, the authorisation.

(5) An authorisation—

(a) may relate to data whether or not in existence at the time of the authorisation,

(b) may authorise the obtaining or disclosure of data by a person who is not an authorised officer, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned, and

(c) may, in particular, require a telecommunications operator who controls or provides a telecommunication system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system.

(6) An authorisation—

(a) may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system, and

(b) may not authorise an authorised officer to ask or require, in the circumstances mentioned in subsection (4)(b) or (c), a person to disclose the data to any person other than—

(i) an authorised officer, or

(ii) an officer of the same relevant public authority as an authorised officer.

(7) It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data—

(a) in the interests of national security,

(b) for the purpose of preventing or detecting crime or of preventing disorder,

(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,

(d) in the interests of public safety,

(e) for the purpose of protecting public health,

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,

(g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,

(h) to assist investigations into alleged miscarriages of justice,

(i) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—

(i) to assist in identifying P, or

(ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition, or

(j) for the purpose of exercising functions relating to—

(i) the regulation of financial services and markets, or

(ii) financial stability.

(8) The fact that the communications data which would be obtained in pursuance of an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that it is necessary to obtain the data for a purpose falling within subsection (7).

(9) See—

(a) sections 70 and 73 for the meanings of "designated senior officer" and "relevant public authority";

(b) section 84 for the way in which this Part applies to postal operators and postal services.

62 Restrictions in relation to internet connection records

(1) A designated senior officer of a local authority may not grant an authorisation for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record.

(2) A designated senior officer of a relevant public authority which is not a local authority may not grant an authorisation for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record unless condition A, B or C is met.

(3) Condition A is that the designated senior officer considers that it is necessary, for a purpose falling within section 61(7), to obtain the data to identify which person or apparatus is using an internet service where—

(a) the service and time of use are already known, but

(b) the identity of the person or apparatus using the service is not known.

(4) Condition B is that—

(a) the purpose for which the data is to be obtained falls within section 61(7) but is not the purpose falling within section 61(7)(b) of preventing or detecting crime, and

(b) the designated senior officer considers that it is necessary to obtain the data to identify—

(i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known,

(ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime, or

(iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(5) Condition C is that—

(a) the purpose for which the data is to be obtained is the purpose falling within section 61(7)(b) of preventing or detecting crime,

(b) the crime to be prevented or detected is serious crime or other relevant crime, and

(c) the designated senior officer considers that it is necessary to obtain the data to identify—

(i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known,

(ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime, or

(iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(6) In subsection (5) "other relevant crime" means crime which is not serious crime but where the offence, or one of the offences, which is or would be constituted by the conduct concerned is—

(a) an offence for which an individual who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) is capable of being sentenced to imprisonment for a term of 12 months or more (disregarding any enactment prohibiting or restricting the imprisonment of individuals who have no previous convictions), or

(b) an offence—

(i) by a person who is not an individual, or

(ii) which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.

(7) In this Act "internet connection record" means communications data which—

(a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

(b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

63 Additional restrictions on grant of authorisations

(1) A designated senior officer may not grant an authorisation for the purposes of a specific investigation or a specific operation if the officer is working on that investigation or operation.

(2) But, if the designated senior officer considers that there are exceptional circumstances which mean that subsection (1) should not apply in a particular case, that subsection does not apply in that case.

(3) Examples of exceptional circumstances include—

(a) an imminent threat to life or another emergency,

(b) the investigation or operation concerned is one where there is an exceptional need, in the interests of national security, to keep knowledge of it to a minimum,

(c) there is an opportunity to obtain information where—

(i) the opportunity is rare,

(ii) the time to act is short, and

(iii) the need to obtain the information is significant and in the interests of national security, or

(d) the size of the relevant public authority concerned is such that it is not practicable to have a designated senior officer who is not working on the investigation or operation concerned.

64 Procedure for authorisations and authorised notices

(1) An authorisation must specify—

(a) the office, rank or position held by the designated senior officer granting it,

(b) the matters falling within section 61(7) by reference to which it is granted,

(c) the conduct that is authorised,

(d) the data or description of data to be obtained, and

(e) the persons or descriptions of persons to whom the data is to be, or may be, disclosed or how to identify such persons.

(2) An authorisation which authorises a person to impose requirements by notice on a telecommunications operator must also specify—

(a) the operator concerned, and

(b) the nature of the requirements that are to be imposed,

but need not specify the other contents of the notice.

(3) The notice itself—

(a) must specify—

(i) the office, rank or position held by the person giving it,

(ii) the requirements that are being imposed, and

(iii) the telecommunications operator on whom the requirements are being imposed, and

(b) must be given in writing or (if not in writing) in a manner that produces a record of its having been given.

(4) An authorisation must be applied for, and granted, in writing or (if not in writing) in a manner that produces a record of its having been applied for or granted.

65 Duration and cancellation of authorisations and notices

(1) An authorisation ceases to have effect at the end of the period of one month beginning with the date on which it is granted.

(2) An authorisation may be renewed at any time before the end of that period by the grant of a further authorisation.

(3) Subsection (1) has effect in relation to a renewed authorisation as if the period of one month mentioned in that subsection did not begin until the end of the period of one month applicable to the authorisation that is current at the time of the renewal.

(4) A designated senior officer who has granted an authorisation—

(a) may cancel it at any time, and

(b) must cancel it if the designated senior officer considers that the requirements of this Part would not be satisfied in relation to granting an equivalent new authorisation.

(5) The Secretary of State may by regulations provide for the person by whom any function under subsection (4) is to be exercised where the person who would otherwise have exercised it is no longer available to do so.

(6) Such regulations may, in particular, provide for the person by whom the function is to be exercised to be a person appointed in accordance with the regulations.

(7) A notice given in pursuance of an authorisation (and any requirement imposed by the notice)—

(a) is not affected by the authorisation subsequently ceasing to have effect under subsection (1), but

(b) is cancelled if the authorisation is cancelled under subsection (4).

66 Duties of telecommunications operators in relation to authorisations

(1) It is the duty of a telecommunications operator on whom a requirement is imposed by notice given in pursuance of an authorisation to comply with that requirement.

(2) It is the duty of a telecommunications operator who is obtaining or disclosing communications data, in response to a request or requirement for the data in pursuance of an authorisation, to obtain or disclose the data in a way that minimises the amount of data that needs to be processed for the purpose concerned.

(3) A person who is under a duty by virtue of subsection (1) or (2) is not required to take any steps in pursuance of that duty which it is not reasonably practicable for that person to take.

(4) For the purposes of subsection (3), where obligations have been imposed on a telecommunications operator ("P") under section 253 (maintenance of technical capability), the steps which it is reasonably practicable for P to take include every step which it would have been reasonably practicable for P to take if P had complied with all of those obligations.

(5) The duty imposed by subsection (1) or (2) is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

Filtering arrangements for obtaining data

67 Filtering arrangements for obtaining data

(1) The Secretary of State may establish, maintain and operate arrangements for the purposes of—

(a) assisting a designated senior officer, who is considering whether to grant an authorisation, to determine whether the requirements of this Part in relation to granting the authorisation are satisfied, or

(b) facilitating the lawful, efficient and effective obtaining of communications data from any person by relevant public authorities in pursuance of an authorisation.

(2) Arrangements under subsection (1) ("filtering arrangements") may, in particular, involve the obtaining of communications data in pursuance of an authorisation ("the target data") by means of—

(a) a request to the Secretary of State to obtain the target data on behalf of an authorised officer, and

(b) the Secretary of State—

(i) obtaining the target data or data from which the target data may be derived,

(ii) processing the target data or the data from which it may be derived (and retaining data temporarily for that purpose), and

(iii) disclosing the target data to the person identified for this purpose by, or in accordance with, the authorisation.

(3) Filtering arrangements may, in particular, involve the generation or use by the Secretary of State of information—

(a) for the purpose mentioned in subsection (1)(a), or

(b) for the purposes of—

(i) the support, maintenance, oversight, operation or administration of the arrangements, or

(ii) the functions of the Investigatory Powers Commissioner mentioned in subsection (4) or (5).

(4) Filtering arrangements must involve the generation and retention of such information or documents as the Investigatory Powers Commissioner considers appropriate for the purposes of the functions of the Commissioner under section 229(1) of keeping under review the exercise by public authorities of functions under this Part.

(5) The Secretary of State must consult the Investigatory Powers Commissioner about the principles on the basis of which the Secretary of State intends to establish, maintain or operate any arrangements for the purpose mentioned in subsection (1)(a).

68 Use of filtering arrangements in pursuance of an authorisation

(1) This section applies in relation to the use of the filtering arrangements in pursuance of an authorisation.

(2) The filtering arrangements may be used—

(a) to obtain and disclose communications data in pursuance of an authorisation, only if the authorisation specifically authorises the use of the arrangements to obtain and disclose the data,

(b) to process data in pursuance of an authorisation (and to retain the data temporarily for that purpose), only if the authorisation specifically authorises processing data of that description under the arrangements (and their temporary retention for that purpose).

(3) An authorisation must record the designated senior officer's decision as to—

(a) whether the communications data to be obtained and disclosed in pursuance of the authorisation may be obtained and disclosed by use of the filtering arrangements,

(b) whether the processing of data under the filtering arrangements (and its temporary retention for that purpose) is authorised,

(c) if the processing of data under the filtering arrangements is authorised, the description of data that may be processed.

(4) A designated senior officer must not grant an authorisation which authorises—

(a) use of the filtering arrangements, or

(b) processing under the filtering arrangements,

unless the condition in subsection (5) is met.

(5) The condition is that the designated senior officer (as well as considering that the other requirements of this Part in relation to granting the authorisation are satisfied) considers that what is authorised in relation to the filtering arrangements is proportionate to what is sought to be achieved.

69 Duties in connection with operation of filtering arrangements

(1) The Secretary of State must secure—

(a) that no authorisation data is obtained or processed under the filtering arrangements except for the purposes of an authorisation,

(b) that data which—

(i) has been obtained or processed under the filtering arrangements, and

(ii) is to be disclosed in pursuance of an authorisation or for the purpose mentioned in section 67(1)(a),

is disclosed only to the person to whom the data is to be disclosed in pursuance of the authorisation or (as the case may be) to the designated senior officer concerned,

(c) that any authorisation data which is obtained under the filtering arrangements in pursuance of an authorisation is immediately destroyed—

(i) when the purposes of the authorisation have been met, or

(ii) if at any time it ceases to be necessary to retain the data for the purposes or purpose concerned.

(2) The Secretary of State must secure that data (other than authorisation data) which is retained under the filtering arrangements is disclosed only—

(a) for the purpose mentioned in section 67(1)(a),

(b) for the purposes of support, maintenance, oversight, operation or administration of the arrangements,

(c) to the Investigatory Powers Commissioner for the purposes of the functions of the Commissioner mentioned in section 67(4) or (5), or

(d) otherwise as authorised by law.

(3) The Secretary of State must secure that—

(a) only the Secretary of State and designated individuals are permitted to read, obtain or otherwise process data for the purposes of support, maintenance, oversight, operation or administration of the filtering arrangements, and

(b) no other persons are permitted to access or use the filtering arrangements except in pursuance of an authorisation or for the purpose mentioned in section 67(1)(a).

(4) In subsection (3)(a) "designated" means designated by the Secretary of State; and the Secretary of State may designate an individual only if the Secretary of State thinks that it is necessary for the individual to be able to act as mentioned in subsection (3)(a).

(5) The Secretary of State must—

(a) put in place and maintain an adequate security system to govern access to, and use of, the filtering arrangements and to protect against any abuse of the power of access, and

(b) impose measures to protect against unauthorised or unlawful data retention, processing, access or disclosure.

(6) The Secretary of State must—

(a) put in place and maintain procedures (including the regular testing of relevant software and hardware) to ensure that the filtering arrangements are functioning properly, and

(b) report, as soon as possible after the end of each calendar year, to the Investigatory Powers Commissioner about the functioning of the filtering arrangements during that year.

(7) A report under subsection (6)(b) must, in particular, contain information about the destruction of authorisation data during the calendar year concerned.

(8) If the Secretary of State believes that significant processing errors have occurred giving rise to a contravention of any of the requirements of this Part which relate to the filtering arrangements, the Secretary of State must report that fact immediately to the Investigatory Powers Commissioner.

(9) In this section "authorisation data", in relation to an authorisation, means communications data that is, or is to be, obtained in pursuance of the authorisation or any data from which that data is, or may be, derived.

Relevant public authorities other than local authorities

70 Relevant public authorities and designated senior officers etc.

(1) Schedule 4 (relevant public authorities and designated senior officers etc.) has effect.

(2) A public authority listed in column 1 of the table in the Schedule is a relevant public authority for the purposes of this Part.

(3) In this Part "designated senior officer", in relation to a relevant public authority listed in column 1 of the table, means an individual who holds with the authority—

(a) an office, rank or position specified in relation to the authority in column 2 of the table, or

(b) an office, rank or position higher than that specified in relation to the authority in column 2 of the table (subject to subsections (4) and (5)).

(4) Subsection (5) applies where an office, rank or position specified in relation to a relevant public authority in column 2 of the table is specified by reference to—

(a) a particular branch, agency or other part of the authority, or

(b) responsibility for functions of a particular description.

(5) A person is a designated senior officer by virtue of subsection (3)(b) only if the person—

(a) holds an office, rank or position in that branch, agency or part, or

(b) has responsibility for functions of that description.

(6) A person who is a designated senior officer of a relevant public authority by virtue of subsection (3) and an entry in column 2 of the table may grant an authorisation—

(a) only for obtaining communications data of the kind specified in the corresponding entry in column 3 of the table, and

(b) only if section 61(1)(a) is met in relation to a purpose within one of the paragraphs of section 61(7) specified in the corresponding entry in column 4 of the table.

(7) Where there is more than one entry in relation to a relevant public authority in column 2 of the table, and a person is a designated senior officer of the authority by virtue of subsection (3) as it applies to more than one of those entries, subsection (6) applies in relation to each entry.

71 Power to modify section 70 and Schedule 4

(1) The Secretary of State may by regulations modify section 70 or Schedule 4.

(2) Regulations under subsection (1) may in particular—

(a) add a public authority to, or remove a public authority from, the list in column 1 of the table,

(b) modify an entry in column 2 of the table,

(c) impose or remove restrictions on the authorisations that may be granted by a designated senior officer with a specified public authority,

(d) impose or remove restrictions on the circumstances in which or purposes for which such authorisations may be granted by a designated senior officer.

(3) The power to make regulations under subsection (1) includes power to make such modifications in any enactment (including this Act) as the Secretary of State considers appropriate in consequence of a person becoming, or ceasing to be, a relevant public authority because of regulations under that subsection.

72 Certain regulations under section 71: supplementary

(1) This section applies to regulations under section 71 other than regulations which do only one or both of the following—

(a) remove a public authority from the list in column 1 of the table in Schedule 4 and make consequential modifications,

(b) modify column 2 of the table in a way that does not involve replacing an office, rank or position specified in that column in relation to a particular public authority with a lower office, rank or position in relation to the same authority.

(2) Before making regulations to which this section applies, the Secretary of State must consult—

(a) the Investigatory Powers Commissioner, and

(b) the public authority to which the modifications relate.

(3) A statutory instrument containing regulations to which this section applies may not be made except in accordance with the enhanced affirmative procedure.

Local authorities

73 Local authorities as relevant public authorities

(1) A local authority is a relevant public authority for the purposes of this Part.

(2) In this Part "designated senior officer", in relation to a local authority, means an individual who holds with the authority—

(a) the position of director, head of service or service manager (or equivalent), or

(b) a higher position.

(3) A designated senior officer of a local authority may grant an authorisation for obtaining communications data only if section 61(1)(a) is met in relation to a purpose within section 61(7)(b).

(4) The Secretary of State may by regulations amend subsection (2).

(5) Before making regulations under subsection (4) which amend subsection (2) so as to replace an office, rank or position specified in that subsection with a lower office, rank or position, the Secretary of State must consult—

(a) the Investigatory Powers Commissioner, and

(b) each local authority to which the amendment relates.

(6) A statutory instrument containing regulations under subsection (4) to which subsection (5) applies may not be made except in accordance with the enhanced affirmative procedure.

(7) Sections 74 and 75 impose further restrictions in relation to the grant of authorisations by local authorities.

74 Requirement to be party to collaboration agreement

(1) A designated senior officer of a local authority may not grant an authorisation unless—

(a) the local authority is a party to a collaboration agreement (whether as a supplying authority or a subscribing authority or both), and

(b) that collaboration agreement is certified by the Secretary of State (having regard to guidance given by virtue of section 79(6) and (7)) as being appropriate for the local authority.

(2) A designated senior officer of a local authority may only grant an authorisation to a person within subsection (3).

(3) A person is within this subsection if the person is an officer of a relevant public authority which is a supplying authority under a collaboration agreement to which the local authority is a party.

(4) If the local authority is itself a supplying authority under a collaboration agreement with the result that officers of the local authority are permitted to be granted authorisations by a designated senior officer of a subscribing authority, the persons within subsection (3) include officers of the local authority.

(5) In this section "collaboration agreement", "subscribing authority" and "supplying authority" have the same meaning as in section 78.

75 Judicial approval for local authority authorisations

(1) This section applies to an authorisation granted by a designated senior officer of a local authority other than an authorisation to which section 77 applies.

(2) The authorisation is not to take effect until such time (if any) as the relevant judicial authority has made an order under this section approving it.

(3) The local authority may apply to the relevant judicial authority for an order under this section approving the authorisation.

(4) The local authority is not required to give notice of the application to—

(a) any person to whom the authorisation relates, or

(b) that person's legal representatives.

(5) The relevant judicial authority may approve the authorisation if, and only if, the relevant judicial authority considers that—

(a) at the time of the grant, there were reasonable grounds for considering that the requirements of this Part were satisfied in relation to the authorisation, and

(b) at the time when the relevant judicial authority is considering the matter, there are reasonable grounds for considering that the requirements of this Part would be satisfied if an equivalent new authorisation were granted at that time.

(6) Where, on an application under this section, the relevant judicial authority refuses to approve the grant of the authorisation, the relevant judicial authority may make an order quashing the authorisation.

(7) In this section "the relevant judicial authority" means—

(a) in relation to England and Wales, a justice of the peace,

(b) in relation to Scotland, a sheriff, and

(c) in relation to Northern Ireland, a district judge (magistrates' courts) in Northern Ireland.

(8) See also sections 77A and 77B of the Regulation of Investigatory Powers Act 2000 (procedure for orders under this section of a sheriff in Scotland or a district judge (magistrates' courts) in Northern Ireland).

Additional protections

76 Use of a single point of contact

(1) Before granting an authorisation, the designated senior officer must consult a person who is acting as a single point of contact in relation to the granting of authorisations.

(2) But, if the designated senior officer considers that there are exceptional circumstances which mean that subsection (1) should not apply in a particular case, that subsection does not apply in that case.

(3) Examples of exceptional circumstances include—

(a) an imminent threat to life or another emergency, or

(b) the interests of national security.

(4) A person is acting as a single point of contact if that person—

(a) is an officer of a relevant public authority, and

(b) is responsible for advising—

(i) officers of the relevant public authority about applying for authorisations, or

(ii) designated senior officers of the relevant public authority about granting authorisations.

(5) A person acting as a single point of contact may, in particular, advise an officer of a relevant public authority who is considering whether to apply for an authorisation about—

(a) the most appropriate methods for obtaining data where the data concerned is processed by more than one telecommunications operator,

(b) the cost, and resource implications, for—

(i) the relevant public authority concerned of obtaining the data, and

(ii) the telecommunications operator concerned of disclosing the data,

(c) any unintended consequences of the proposed authorisation, and

(d) any issues as to the lawfulness of the proposed authorisation.

(6) A person acting as a single point of contact may, in particular, advise a designated senior officer who is considering whether to grant an authorisation about—

(a) whether it is reasonably practical to obtain the data sought in pursuance of the proposed authorisation,

(b) the cost, and resource implications, for—

(i) the relevant public authority concerned of obtaining the data, and

(ii) the telecommunications operator concerned of disclosing the data,

(c) any unintended consequences of the proposed authorisation, and

(d) any issues as to the lawfulness of the proposed authorisation.

(7) A person acting as a single point of contact may also provide advice about—

(a) whether requirements imposed by virtue of an authorisation have been met,

(b) the use in support of operations or investigations of communications data obtained in pursuance of an authorisation, and

(c) any other effects of an authorisation.

(8) Nothing in this section prevents a person acting as a single point of contact from also applying for, or being granted, an authorisation or, in the case of a designated senior officer, granting an authorisation.

77 Commissioner approval for authorisations to identify or confirm journalistic sources

(1) Subsection (2) applies if—

(a) a designated senior officer has granted an authorisation in relation to the obtaining by a relevant public authority of communications data for the purpose of identifying or confirming a source of journalistic information, and

(b) the authorisation is not necessary because of an imminent threat to life.

(2) The authorisation is not to take effect until such time (if any) as a Judicial Commissioner has approved it.

(3) The relevant public authority for which the authorisation has been granted may apply to a Judicial Commissioner for approval of the authorisation.

(4) The applicant is not required to give notice of the application to—

(a) any person to whom the authorisation relates, or

(b) that person's legal representatives.

(5) A Judicial Commissioner may approve the authorisation if, and only if, the Judicial Commissioner considers that—

(a) at the time of the grant, there were reasonable grounds for considering that the requirements of this Part were satisfied in relation to the authorisation, and

(b) at the time when the Judicial Commissioner is considering the matter, there are reasonable grounds for considering that the requirements of this Part would be satisfied if an equivalent new authorisation were granted at that time.

(6) In considering whether the position is as mentioned in subsection (5)(a) and (b), the Judicial Commissioner must, in particular, have regard to—

(a) the public interest in protecting a source of journalistic information, and

(b) the need for there to be another overriding public interest before a relevant public authority seeks to identify or confirm a source of journalistic information.

(7) Where, on an application under this section, the Judicial Commissioner refuses to approve the grant of the authorisation, the Judicial Commissioner may quash the authorisation.

Collaboration agreements

78 Collaboration agreements

(1) A collaboration agreement is an agreement (other than a police collaboration agreement) under which—

(a) a relevant public authority ("the supplying authority") puts the services of designated senior officers of that authority or other officers of that authority at the disposal of another relevant public authority ("the subscribing authority") for the purposes of the subscribing authority's functions under this Part, and

(b) either—

(i) a designated senior officer of the supplying authority is permitted to grant authorisations to officers of the subscribing authority,

(ii) officers of the supplying authority are permitted to be granted authorisations by a designated senior officer of the subscribing authority, or

(iii) officers of the supplying authority act as single points of contact for officers of the subscribing authority.

(2) The persons by whom, or to whom, authorisations may be granted (or who may act as single points of contact) under a collaboration agreement are additional to those persons by whom, or to whom, authorisations would otherwise be granted under this Part (or who could otherwise act as single points of contact).

(3) In a case falling within subsection (1)(b)(i)—

(a) section 61 has effect as if—

(i) in subsection (2) the reference to an officer of the authority were a reference to an officer of the subscribing authority, and

(ii) in subsection (6)(b)(ii) the reference to an officer of the same relevant public authority as an authorised officer included a reference to an officer of the supplying authority,

(b) section 63(3)(d) has effect as if the reference to the relevant public authority concerned were a reference to both authorities,

(c) this Part has effect as if the designated senior officer of the supplying authority had the power to grant an authorisation to officers of the subscribing authority, and had other functions in relation to the authorisation, which were the same as (and subject to no greater or lesser restrictions than) the power and other functions which the designated senior officer of the subscribing authority who would otherwise have dealt with the authorisation would have had, and

(d) section 75(1) applies to the authorisation as if it were granted by a designated senior officer of the subscribing authority.

(4) In a case falling within subsection (1)(b)(ii)—

(a) section 61 has effect as if—

(i) in subsection (2) the reference to an officer of the authority were a reference to an officer of the supplying authority, and

(ii) in subsection (6)(b)(ii) the reference to an officer of the same relevant public authority as an authorised officer included a reference to an officer of the subscribing authority, and

(b) section 63(3)(d) has effect as if the reference to the relevant public authority concerned were a reference to both authorities.

(5) In a case falling within subsection (1)(b)(iii), section 76(4)(b) has effect as if the references to the relevant public authority were references to the subscribing authority.

(6) In this section—

"force collaboration provision" has the meaning given by paragraph (a) of section 22A(2) of the Police Act 1996 but as if the reference in that paragraph to a police force included the National Crime Agency,

"police collaboration agreement" means a collaboration agreement under section 22A of the Police Act 1996 which contains force collaboration provision.

79 Collaboration agreements: supplementary

(1) A collaboration agreement may provide for payments to be made between parties to the agreement.

(2) A collaboration agreement—

(a) must be in writing,

(b) may be varied by a subsequent collaboration agreement, and

(c) may be brought to an end by agreement between the parties to it.

(3) A person who makes a collaboration agreement must—

(a) publish the agreement, or

(b) publish the fact that the agreement has been made and such other details about it as the person considers appropriate.

(4) A relevant public authority may enter into a collaboration agreement as a supplying authority, a subscribing authority or both (whether or not it would have power to do so apart from this section).

(5) The Secretary of State may, after consulting a relevant public authority, direct it to enter into a collaboration agreement if the Secretary of State considers that entering into the agreement would assist the effective exercise by the authority, or another relevant public authority, of its functions under this Part.

(6) A code of practice under Schedule 7 must include guidance to relevant public authorities about collaboration agreements.

(7) The guidance must include guidance about the criteria the Secretary of State will use in considering whether a collaboration agreement is appropriate for a relevant public authority.

80 Police collaboration agreements

(1) This section applies if—

(a) the chief officer of police of an England and Wales police force ("force 1") has entered into a police collaboration agreement for the purposes of a collaborating police force's functions under this Part, and

(b) under the terms of the agreement—

(i) a designated senior officer of force 1 is permitted to grant authorisations to officers of the collaborating police force,

(ii) officers of force 1 are permitted to be granted authorisations by a designated senior officer of the collaborating police force, or

(iii) officers of force 1 act as single points of contact for officers of the collaborating police force.

(2) The persons by whom, or to whom, authorisations may be granted (or who may act as single points of contact) under a police collaboration agreement are additional to those persons by whom, or to whom, authorisations would otherwise be granted under this Part (or who could otherwise act as single points of contact).

(3) In a case falling within subsection (1)(b)(i)—

(a) section 61 has effect as if—

(i) in subsection (2) the reference to an officer of the authority were a reference to an officer of the collaborating police force, and

(ii) in subsection (6)(b)(ii) the reference to an officer of the same relevant public authority as an authorised officer included a reference to an officer of force 1,

(b) section 63(3)(d) has effect as if the reference to the relevant public authority concerned were a reference to force 1 and the collaborating police force, and

(c) this Part has effect as if the designated senior officer of force 1 had the power to grant an authorisation to officers of the collaborating police force, and had other functions in relation to the authorisation, which were the same as (and subject to no greater or lesser restrictions than) the power and other functions which the designated senior officer of the collaborating police force who would otherwise have dealt with the authorisation would have had.

(4) In a case falling within subsection (1)(b)(ii)—

(a) section 61 has effect as if—

(i) in subsection (2) the reference to an officer of the authority were a reference to an officer of force 1, and

(ii) in subsection (6)(b)(ii) the reference to an officer of the same relevant public authority as an authorised officer included a reference to an officer of the collaborating police force, and

(b) section 63(3)(d) has effect as if the reference to the relevant public authority concerned were a reference to force 1 and the collaborating police force.

(5) In a case falling within subsection (1)(b)(iii), section 76(4)(b) has effect as if the references to the relevant public authority were references to the collaborating police force.

(6) In this section—

"collaborating police force", in relation to a police collaboration agreement, means a police force (other than force 1) whose chief officer of police is a party to the agreement,

"England and Wales police force" means—

(a) any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London),

(b) the metropolitan police force, or

(c) the City of London police force,

"police collaboration agreement" has the same meaning as in section 78 (see subsection (6) of that section),

and references in this section to an England and Wales police force or a police force include the National Crime Agency (and references to the chief officer of police include the Director General of the National Crime Agency).

Further and supplementary provision

81 Lawfulness of conduct authorised by this Part

(1) Conduct is lawful for all purposes if—

(a) it is conduct in which any person is authorised to engage by an authorisation or required to undertake by virtue of a notice given in pursuance of an authorisation, and

(b) the conduct is in accordance with, or in pursuance of, the authorisation or notice.

(2) A person (whether or not the person so authorised or required) is not to be subject to any civil liability in respect of conduct that—

(a) is incidental to, or is reasonably undertaken in connection with, conduct that is lawful by virtue of subsection (1), and

(b) is not itself conduct for which an authorisation or warrant—

(i) is capable of being granted under any of the enactments mentioned in subsection (3), and

(ii) might reasonably have been expected to have been sought in the case in question.

(3) The enactments referred to in subsection (2)(b)(i) are—

(a) an enactment contained in this Act,

(b) an enactment contained in the Regulation of Investigatory Powers Act 2000,

(c) an enactment contained in Part 3 of the Police Act 1997 (powers of the police and of customs officers), or

(d) section 5 of the Intelligence Services Act 1994 (warrants for the intelligence services).

82 Offence of making unauthorised disclosure

(1) It is an offence for a telecommunications operator, or any person employed or engaged for the purposes of the business of a telecommunications operator, to disclose, without reasonable excuse, to any person the existence of—

(a) any requirement imposed on the operator by virtue of this Part to disclose communications data relating to that person, or

(b) any request made in pursuance of an authorisation for the operator to disclose such data.

(2) For the purposes of subsection (1), it is, in particular, a reasonable excuse if the disclosure is made with the permission of the relevant public authority which is seeking to obtain the data from the operator (whether the permission is contained in any notice requiring the operator to disclose the data or otherwise).

(3) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

83 Certain transfer and agency arrangements with public authorities

(1) The Secretary of State may by regulations provide for—

(a) any function under sections 67 to 69 which is exercisable by the Secretary of State to be exercisable instead by another public authority, or

(b) any function under sections 67 to 69 which is exercisable by a public authority by virtue of paragraph (a) to be exercisable instead by the Secretary of State.

(2) The Secretary of State may by regulations modify any enactment about a public authority for the purpose of enabling or otherwise facilitating any function exercisable by the Secretary of State under this Part to be exercisable on behalf of the Secretary of State by the authority concerned.

(3) Regulations under subsection (2) do not affect the Secretary of State's responsibility for the exercise of the functions concerned.

(4) Subsection (2) does not apply in relation to any function of the Secretary of State of making regulations.

(5) Schedule 5 (which contains further safeguards and provisions supplementing this section) has effect.

84 Application of Part 3 to postal operators and postal services

(1) This Part applies to postal operators and postal services as it applies to telecommunications operators and telecommunications services.

(2) In its application by virtue of subsection (1), this Part has effect as if—

(a) any reference to a telecommunications operator were a reference to a postal operator,

(b) any reference to a telecommunications service were a reference to a postal service,

(c) any reference to a telecommunication system were a reference to a postal service,

(d) sections 61(3)(a) and 62 were omitted, and

(e) in Part 2 of Schedule 4, for "which is entity data" there were substituted "within paragraph (c) of the definition of "communications data" in section 262(3)".

85 Extra-territorial application of Part 3

(1) An authorisation may relate to conduct outside the United Kingdom and persons outside the United Kingdom.

(2) A notice given in pursuance of an authorisation may relate to conduct outside the United Kingdom and persons outside the United Kingdom.

(3) Where such a notice is to be given to a person outside the United Kingdom, the notice may be given to the person in any of the following ways (as well as by electronic or other means of service)—

(a) by delivering it to the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, to any place in the United Kingdom where the person carries on business or conducts activities,

(b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept documents of the same description as a notice, by delivering it to that address,

(c) by notifying the person by such other means as the authorised officer considers appropriate (which may include notifying the person orally).

(4) In determining for the purposes of subsection (3) of section 66 whether it is reasonably practicable for a telecommunications operator outside the United Kingdom to take

any steps in a country or territory outside the United Kingdom for the purpose of complying with a duty imposed by virtue of subsection (1) or (2) of that section, the matters to be taken into account include the following—

(a) any requirements or restrictions under the law of that country or territory that are relevant to the taking of those steps, and

(b) the extent to which it is reasonably practicable to comply with the duty in a way that does not breach any of those requirements or restrictions.

(5) Nothing in the definition of "telecommunications operator" limits the type of communications data in relation to which an authorisation, or a request or requirement of a kind which gives rise to a duty under section 66(1) or (2), may apply.

86 Part 3: interpretation

(1) In this Part—

"authorisation" means an authorisation under section 61 (including that section as modified by sections 78 and 80),

"designated senior officer"—

(a) in relation to a relevant public authority which is a local authority, has the meaning given by section 73(2), and

(b) in relation to any other relevant public authority, has the meaning given by section 70(3),

"filtering arrangements" means any arrangements under section 67(1),

"officer", in relation to a relevant public authority, means a person holding an office, rank or position with that authority,

"relevant public authority" means a public authority which is a relevant public authority for the purposes of this Part by virtue of section 70(2) or 73(1).

(2) In this Part "local authority" means—

(a) a district or county council in England,

(b) a London borough council,

(c) the Common Council of the City of London in its capacity as a local authority,

(d) the Council of the Isles of Scilly,

(e) a county council or county borough council in Wales,

(f) a council constituted under section 2 of the Local Government etc. (Scotland) Act 1994, and

(g) a district council in Northern Ireland.

(3) See also—

section 261 (telecommunications definitions),

section 262 (postal definitions),

section 263 (general definitions),

section 265 (index of defined expressions).

PART 4

RETENTION OF COMMUNICATIONS DATA

General

87 Powers to require retention of certain data

(1) The Secretary of State may, by notice (a "retention notice") and subject as follows, require a telecommunications operator to retain relevant communications data if—

(a) the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7) (purposes for which communications data may be obtained), and

(b) the decision to give the notice has been approved by a Judicial Commissioner.

(2) A retention notice may—

(a) relate to a particular operator or any description of operators,

(b) require the retention of all data or any description of data,

(c) identify the period or periods for which data is to be retained,

(d) contain other requirements, or restrictions, in relation to the retention of data,

(e) make different provision for different purposes,

(f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.

(3) A retention notice must not require any data to be retained for more than 12 months beginning with—

(a) in the case of communications data relating to a specific communication, the day of the communication concerned,

(b) in the case of entity data which does not fall within paragraph (a) above but does fall within paragraph (a)(i) of the definition of "communications data" in section 261(5), the day on which the entity concerned ceases to be associated with the telecommunications service concerned or (if earlier) the day on which the data is changed, and

(c) in any other case, the day on which the data is first held by the operator concerned.

(4) A retention notice must not require an operator who controls or provides a telecommunication system ("the system operator") to retain data which—

(a) relates to the use of a telecommunications service provided by another telecommunications operator in relation to that system,

(b) is (or is capable of being) processed by the system operator as a result of being comprised in, included as part of, attached to or logically associated with a communication transmitted by means of the system as a result of the use mentioned in paragraph (a),

(c) is not needed by the system operator for the functioning of the system in relation to that communication, and

(d) is not retained or used by the system operator for any other lawful purpose,

and which it is reasonably practicable to separate from other data which is subject to the notice.

(5) A retention notice which relates to data already in existence when the notice comes into force imposes a requirement to retain the data for only so much of a period of retention as occurs on or after the coming into force of the notice.

(6) A retention notice comes into force—

(a) when the notice is given to the operator (or description of operators) concerned, or

(b) (if later) at the time or times specified in the notice.

(7) A retention notice is given to an operator (or description of operators) by giving, or publishing, it in such manner as the Secretary of State considers appropriate for bringing it to the attention of the operator (or description of operators) to whom it relates.

(8) A retention notice must specify—

(a) the operator (or description of operators) to whom it relates,

(b) the data which is to be retained,

(c) the period or periods for which the data is to be retained,

(d) any other requirements, or any restrictions, in relation to the retention of the data,

(e) the information required by section 249(7) (the level or levels of contribution in respect of costs incurred as a result of the notice).

(9) The requirements or restrictions mentioned in subsection (8)(d) may, in particular, include—

(a) a requirement to retain the data in such a way that it can be transmitted efficiently and effectively in response to requests,

(b) requirements or restrictions in relation to the obtaining (whether by collection, generation or otherwise), generation or processing of—

(i) data for retention, or

(ii) retained data.

(10) The fact that the data which would be retained under a retention notice relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the requirement to retain the data is necessary for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7).

(11) In this Part "relevant communications data" means communications data which may be used to identify, or assist in identifying, any of the following—

(a) the sender or recipient of a communication (whether or not a person),

(b) the time or duration of a communication,

(c) the type, method or pattern, or fact, of communication,

(d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted, or

(e) the location of any such system,

and this expression therefore includes, in particular, internet connection records.

Safeguards

88 Matters to be taken into account before giving retention notices

(1) Before giving a retention notice, the Secretary of State must, among other matters, take into account—

(a) the likely benefits of the notice,

(b) the likely number of users (if known) of any telecommunications service to which the notice relates,

(c) the technical feasibility of complying with the notice,

(d) the likely cost of complying with the notice, and

(e) any other effect of the notice on the telecommunications operator (or description of operators) to whom it relates.

(2) Before giving such a notice, the Secretary of State must take reasonable steps to consult any operator to whom it relates.

89 Approval of retention notices by Judicial Commissioners

(1) In deciding whether to approve a decision to give a retention notice, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the requirement to be imposed by the notice to retain relevant communications data is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7).

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to give a retention notice, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to give a retention notice, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to give the notice.

90 Review by the Secretary of State

(1) A telecommunications operator to whom a retention notice is given may, within such period or circumstances as may be provided for by regulations made by the Secretary of State, refer the notice back to the Secretary of State.

(2) Such a reference may be in relation to the whole of a notice or any aspect of it.

(3) In the case of a notice given to a description of operators—

(a) each operator falling within that description may make a reference under subsection (1), but

(b) each such reference may only be in relation to the notice, or aspect of the notice, so far as it applies to that operator.

(4) There is no requirement for an operator who has referred a retention notice under subsection (1) to comply with the notice, so far as referred, until the Secretary of State has reviewed the notice in accordance with subsection (5).

(5) The Secretary of State must review any notice so far as referred to the Secretary of State under subsection (1).

(6) Before deciding the review, the Secretary of State must consult—

(a) the Technical Advisory Board, and

(b) a Judicial Commissioner.

(7) The Board must consider the technical requirements and the financial consequences, for the operator who has made the reference, of the notice so far as referred.

(8) The Commissioner must consider whether the notice so far as referred is proportionate.

(9) The Board and the Commissioner must—

(a) give the operator concerned and the Secretary of State the opportunity to provide evidence, or make representations, to them before reaching their conclusions, and

(b) report their conclusions to—

(i) the operator, and

(ii) the Secretary of State.

(10) The Secretary of State may, after considering the conclusions of the Board and the Commissioner—

(a) vary or revoke the retention notice under section 94, or

(b) give a notice under this section to the operator concerned confirming its effect.

(11) But the Secretary of State may vary the notice, or give a notice under subsection (10)(b) confirming its effect, only if the Secretary of State's decision to do so has been approved by the Investigatory Powers Commissioner.

(12) A report or notice under this section is given to an operator by giving or publishing it in such manner as the Secretary of State considers appropriate for bringing it to the attention of the operator.

(13) The Secretary of State must keep a retention notice under review (whether or not referred under subsection (1)).

91 Approval of notices following review under section 90

(1) In deciding whether to approve a decision to vary a retention notice as mentioned in section 90(10)(a), or to give a notice under section 90(10)(b) confirming the effect of a retention notice, the Investigatory Powers Commissioner must review the Secretary of State's conclusions as to whether the requirement to be imposed by the notice as varied or confirmed to retain relevant communications data is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7).

(2) In doing so, the Investigatory Powers Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Investigatory Powers Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where the Investigatory Powers Commissioner refuses to approve a decision to vary a retention notice as mentioned in section 90(10)(a), or to give a notice under section 90(10)(b) confirming the effect of a retention notice, the Investigatory Powers Commissioner must give the Secretary of State written reasons for the refusal.

92 Data integrity and security

(1) A telecommunications operator who retains relevant communications data by virtue of this Part must—

(a) secure that the data is of the same integrity, and subject to at least the same security and protection, as the data on any system from which it is derived,

(b) secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and

(c) protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure.

(2) A telecommunications operator who retains relevant communications data by virtue of this Part must destroy the data if the retention of the data ceases to be authorised by virtue of this Part and is not otherwise authorised by law.

(3) The destruction of the data may take place at such monthly or shorter intervals as appear to the operator to be practicable.

93 Disclosure of retained data

A telecommunications operator must put in place adequate security systems (including technical and organisational measures) governing access to relevant communications data retained by virtue of this Part in order to protect against any unlawful disclosure.

Variation or revocation of notices

94 Variation or revocation of notices

(1) The Secretary of State may vary a retention notice.

(2) The Secretary of State must give, or publish, notice of the variation in such manner as the Secretary of State considers appropriate for bringing the variation to the attention of the telecommunications operator (or description of operators) to whom it relates.

(3) A variation comes into force—

(a) when notice of it is given or published in accordance with subsection (2), or

(b) (if later) at the time or times specified in the notice of variation.

(4) A retention notice may not be varied so as to require the retention of additional relevant communications data unless—

(a) the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7), and

(b) subject to subsection (6), the decision to vary the notice has been approved by a Judicial Commissioner.

(5) The fact that additional relevant communications data which would be retained under a retention notice as varied relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the requirement to retain the data is necessary for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7).

(6) Subsection (4)(b) does not apply to a variation to which section 90(11) applies.

(7) Section 87(2) and (5) apply in relation to a retention notice as varied as they apply in relation to a retention notice, but as if the references to the notice coming into force included references to the variation coming into force.

(8) Sections 87(3), (4) and (8), 95 and 97, and subsections (1), (4), (13) and (16) of this section, apply in relation to a retention notice as varied as they apply in relation to a retention notice.

(9) Section 88 applies in relation to the making of a variation as it applies in relation to the giving of a retention notice (and, accordingly, the references to the notice in section 88(1)(a) to (e) are to be read as references to the variation).

(10) Section 89 applies in relation to a decision to vary to which subsection (4)(b) above applies as it applies in relation to a decision to give a retention notice (and, accordingly, the reference in subsection (1) of that section to the requirement to be imposed by the notice is to be read as a reference to the requirement to be imposed by the variation).

(11) Section 90 applies (but only so far as the variation is concerned) in relation to a retention notice as varied (other than one varied as mentioned in subsection (10)(a) of that section) as it applies in relation to a retention notice.

(12) Section 91 applies in relation to a decision under section 90(10) to vary or confirm a variation as it applies in relation to a decision to vary or confirm a retention notice (and, accordingly, the reference in subsection (1) of that section to the requirement to be imposed by the notice as varied or confirmed is to be read as a reference to the requirement to be imposed by the variation as varied or confirmed).

(13) The Secretary of State may revoke (whether wholly or in part) a retention notice.

(14) The Secretary of State must give or publish notice of the revocation in such manner as the Secretary of State considers appropriate for bringing the revocation to the attention of the operator (or description of operators) to whom it relates.

(15) A revocation comes into force—

(a) when notice of it is given or published in accordance with subsection (14), or

(b) (if later) at the time or times specified in the notice of revocation.

(16) The fact that a retention notice has been revoked in relation to a particular description of communications data and a particular operator (or description of operators) does not prevent the giving of another retention notice in relation to the same description of data and the same operator (or description of operators).

Enforcement

95 Enforcement of notices and certain other requirements and restrictions

(1) It is the duty of a telecommunications operator on whom a requirement or restriction is imposed by—

(a) a retention notice, or

(b) section 92 or 93,

to comply with the requirement or restriction.

(2) A telecommunications operator, or any person employed or engaged for the purposes of the business of a telecommunications operator, must not disclose the existence or contents of a retention notice to any other person.

(3) The Information Commissioner, or any member of staff of the Information Commissioner, must not disclose the existence or contents of a retention notice to any other person.

(4) Subsections (2) and (3) do not apply to a disclosure made with the permission of the Secretary of State.

(5) The duty under subsection (1) or (2) is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

Further and supplementary provision

96 Application of Part 4 to postal operators and postal services

(1) This Part applies to postal operators and postal services as it applies to telecommunications operators and telecommunications services.

(2) In its application by virtue of subsection (1), this Part has effect as if—

(a) any reference to a telecommunications operator were a reference to a postal operator,

(b) any reference to a telecommunications service were a reference to a postal service,

(c) any reference to a telecommunication system were a reference to a postal service,

(d) in section 87(3), for paragraph (b) there were substituted—

"(b) in the case of communications data which does not fall within paragraph (a) above but does fall within paragraph (c) of the definition of "communications data" in section 262(3), the day on which the person concerned leaves the postal service concerned or (if earlier) the day on which the data is changed,",

(e) for section 87(4) there were substituted—

"(4) A retention notice must not require an operator who provides a postal service ("the network operator") to retain data which—

(a) relates to the use of a postal service provided by another postal operator in relation to the postal service of the network operator,

(b) is (or is capable of being) processed by the network operator as a result of being comprised in, included as part of, attached to or logically associated with a communication transmitted by means of the postal service of the network operator as a result of the use mentioned in paragraph (a),

(c) is not needed by the network operator for the functioning of the network operator's postal service in relation to that communication, and

(d) is not retained or used by the network operator for any other lawful purpose,

and which it is reasonably practicable to separate from other data which is subject to the notice.", and

(f) in section 87(11), the words from "and this expression" to the end were omitted.

97 Extra-territorial application of Part 4

(1) A retention notice, and any requirement or restriction imposed by virtue of a retention notice or by section 92, 93 or 95(1) to (3), may relate to conduct outside the United Kingdom and persons outside the United Kingdom.

(2) But section 95(5), so far as relating to those requirements or restrictions, does not apply to a person outside the United Kingdom.

98 Part 4: interpretation

(1) In this Part—

"notice" means notice in writing,

"relevant communications data" has the meaning given by section 87(11),

"retention notice" has the meaning given by section 87(1).

(2) See also—

section 261 (telecommunications definitions),
section 262 (postal definitions),
section 263 (general definitions),
section 265 (index of defined expressions).

PART 5

EQUIPMENT INTERFERENCE

Warrants under this Part

99 Warrants under this Part: general

(1) There are two kinds of warrants which may be issued under this Part—

(a) targeted equipment interference warrants (see subsection (2));

(b) targeted examination warrants (see subsection (9)).

(2) A targeted equipment interference warrant is a warrant which authorises or requires the person to whom it is addressed to secure interference with any equipment for the purpose of obtaining—

(a) communications (see section 135);

(b) equipment data (see section 100);

(c) any other information.

(3) A targeted equipment interference warrant—

(a) must also authorise or require the person to whom it is addressed to secure the obtaining of the communications, equipment data or other information to which the warrant relates;

(b) may also authorise that person to secure the disclosure, in any manner described in the warrant, of anything obtained under the warrant by virtue of paragraph (a).

(4) The reference in subsections (2) and (3) to the obtaining of communications or other information includes doing so by—

(a) monitoring, observing or listening to a person's communications or other activities;

(b) recording anything which is monitored, observed or listened to.

(5) A targeted equipment interference warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including conduct for securing the obtaining of communications, equipment data or other information;

(b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant.

(6) A targeted equipment interference warrant may not, by virtue of subsection (3), authorise or require a person to engage in conduct, in relation to a communication other than a stored communication, which would (unless done with lawful authority) constitute an offence under section 3(1) (unlawful interception).

(7) Subsection (5)(a) does not authorise a person to engage in conduct which could not be expressly authorised under the warrant because of the restriction imposed by subsection (6).

(8) In subsection (6), "stored communication" means a communication stored in or by a telecommunication system (whether before or after its transmission).

(9) A targeted examination warrant is a warrant which authorises the person to whom it is addressed to carry out the selection of protected material obtained under a bulk equipment interference warrant for examination, in breach of the prohibition in section 193(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands).

In this Part, "protected material", in relation to a targeted examination warrant, means any material obtained under a bulk equipment interference warrant under Chapter 3 of Part 6, other than material which is—

(a) equipment data;
(b) information (other than a communication or equipment data) which is not private information.

(10) For provision enabling the combination of targeted equipment interference warrants with certain other warrants or authorisations (including targeted examination warrants), see Schedule 8.

(11) Any conduct which is carried out in accordance with a warrant under this Part is lawful for all purposes.

100 Meaning of "equipment data"

(1) In this Part, "equipment data" means—
(a) systems data;
(b) data which falls within subsection (2).

(2) The data falling within this subsection is identifying data which—
(a) is, for the purposes of a relevant system, comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) or any other item of information,
(b) is capable of being logically separated from the remainder of the communication or the item of information, and
(c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication or the item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact.

(3) In subsection (2), "relevant system" means any system on or by means of which the data is held.

(4) For the meaning of "systems data" and "identifying data", see section 263.

101 Subject-matter of warrants

(1) A targeted equipment interference warrant may relate to any one or more of the following matters—
(a) equipment belonging to, used by or in the possession of a particular person or organisation;
(b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;
(c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;
(d) equipment in a particular location;
(e) equipment in more than one location, where the interference is for the purpose of a single investigation or operation;
(f) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description;

(g) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information;

(h) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment.

(2) A targeted examination warrant may relate to any one or more of the following matters—

(a) a particular person or organisation;

(b) a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;

(c) more than one person or organisation, where the conduct authorised by the warrant is for the purpose of a single investigation or operation;

(d) the testing, maintenance or development of capabilities relating to the selection of protected material for examination;

(e) the training of persons who carry out, or are likely to carry out, the selection of such material for examination.

Power to issue warrants

102 Power to issue warrants to intelligence services: the Secretary of State

(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted equipment interference warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (5),

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 129 and 130 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(2) But the Secretary of State may not issue a targeted equipment interference warrant under subsection (1) if—

(a) the Secretary of State considers that the only ground for considering the warrant to be necessary is for the purpose of preventing or detecting serious crime, and

(b) the warrant, if issued, would authorise interference only with equipment which would be in Scotland at the time of the issue of the warrant or which the Secretary of State believes would be in Scotland at that time.

For the power of the Scottish Ministers to issue a targeted equipment interference warrant, see section 103.

(3) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (5),

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that the warrant is or may be necessary to authorise the selection of protected material for examination in breach of the prohibition in section 193(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands), and

(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(4) But the Secretary of State may not issue a targeted examination warrant under subsection (3) if the warrant, if issued, would relate only to a person who would be in Scotland at the time of the issue of the warrant or whom the Secretary of State believes would be in Scotland at that time.

For the power of the Scottish Ministers to issue a targeted examination warrant, see section 103.

(5) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security,

(b) for the purpose of preventing or detecting serious crime, or

(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.

(6) A warrant may be considered necessary on the ground falling within subsection (5)(c) only if the interference with equipment which would be authorised by the warrant is considered necessary for the purpose of obtaining information relating to the acts or intentions of persons outside the British Islands.

(7) The fact that the information which would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on grounds falling within subsection (5).

(8) An application for the issue of a warrant under this section may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

(9) Nothing in subsection (2) or (4) prevents the Secretary of State from doing anything under this section for the purposes specified in section 2(2) of the European Communities Act 1972.

103 Power to issue warrants to intelligence services: the Scottish Ministers

(1) The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a targeted equipment interference warrant if—

(a) the warrant authorises interference only with equipment which is in Scotland at the time the warrant is issued or which the Scottish Ministers believe to be in Scotland at that time,

(b) the Scottish Ministers consider that the warrant is necessary for the purpose of preventing or detecting serious crime,

(c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) the Scottish Ministers consider that satisfactory arrangements made for the purposes of sections 129 and 130 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(e) except where the Scottish Ministers consider that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(2) The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—

(a) the warrant relates only to a person who is in Scotland, or whom the Scottish Ministers believe to be in Scotland, at the time of the issue of the warrant,

(b) the Scottish Ministers consider that the warrant is necessary for the purpose of preventing or detecting serious crime,

(c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) the Scottish Ministers consider that the warrant is or may be necessary to authorise the selection of protected material in breach of the prohibition in section 193(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands), and

(e) except where the Scottish Ministers consider that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(3) The fact that the information which would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary as mentioned in subsection (1)(b) or (2)(b).

(4) An application for the issue of a warrant under this section may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

104 Power to issue warrants to the Chief of Defence Intelligence

(1) The Secretary of State may, on an application made by or on behalf of the Chief of Defence Intelligence, issue a targeted equipment interference warrant if—

(a) the Secretary of State considers that the warrant is necessary in the interests of national security,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 129 and 130 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(2) The fact that the information which would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary as mentioned in subsection (1)(a).

(3) An application for the issue of a warrant under this section may only be made on behalf of the Chief of Defence Intelligence by a person holding office under the Crown.

105 Decision to issue warrants under sections 102 to 104 to be taken personally by Ministers

(1) The decision to issue a warrant under section 102 or 104 must be taken personally by the Secretary of State.

(2) The decision to issue a warrant under section 103 must be taken personally by a member of the Scottish Government.

(3) Before a warrant under section 102, 103 or 104 is issued, it must be signed by the person who has taken the decision to issue it (subject to subsection (4)).

(4) If it is not reasonably practicable for a warrant to be signed by the person who has taken the decision to issue it, the warrant may be signed by a senior official designated by the Secretary of State or (as the case may be) the Scottish Ministers for that purpose.

(5) In such a case, the warrant must contain a statement that—

(a) it is not reasonably practicable for the warrant to be signed by the person who took the decision to issue it, and

(b) the Secretary of State or (as the case may be) a member of the Scottish Government has personally and expressly authorised the issue of the warrant.

106 Power to issue warrants to law enforcement officers

(1) A law enforcement chief described in Part 1 or 2 of the table in Schedule 6 may, on an application made by a person who is an appropriate law enforcement officer in relation to the chief, issue a targeted equipment interference warrant if—

(a) the law enforcement chief considers that the warrant is necessary for the purpose of preventing or detecting serious crime,

(b) the law enforcement chief considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the law enforcement chief considers that satisfactory arrangements made for the purposes of sections 129 and 130 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(d) except where the law enforcement chief considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(2) The fact that the information which would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary as mentioned in subsection (1)(a).

(3) A law enforcement chief described in Part 1 of the table in Schedule 6 may, on an application made by a person who is an appropriate law enforcement officer in relation to the chief, issue a targeted equipment interference warrant if—

(a) the law enforcement chief considers that the warrant is necessary for the purpose of preventing death or any injury or damage to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health,

(b) the law enforcement chief considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the law enforcement chief considers that satisfactory arrangements made for the purposes of sections 129 and 130 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(d) except where the law enforcement chief considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(4) If it is not reasonably practicable for a law enforcement chief to consider an application under this section, an appropriate delegate may, in an urgent case, exercise the power to issue a targeted equipment interference warrant.

(5) For the purposes of this section—

(a) a person is a law enforcement chief if the person is listed in the first column of the table in Schedule 6;

(b) a person is an appropriate delegate in relation to a law enforcement chief listed in the first column if the person is listed in the corresponding entry in the second column of that table;

(c) a person is an appropriate law enforcement officer in relation to a law enforcement chief listed in the first column if the person is listed in the corresponding entry in the third column of that table.

(6) Where the law enforcement chief is the Chief Constable or the Deputy Chief Constable of the Police Service of Northern Ireland, the reference in subsection (1)(a) to the purpose of preventing or detecting serious crime includes a reference to the interests of national security.

(7) A law enforcement chief who is an immigration officer may consider that the condition in subsection (1)(a) is satisfied only if the serious crime relates to an offence which is an immigration or nationality offence (whether or not it also relates to other offences).

(8) A law enforcement chief who is an officer of Revenue and Customs may consider that the condition in subsection (1)(a) is satisfied only if the serious crime relates to an assigned matter within the meaning of section 1(1) of the Customs and Excise Management Act 1979.

(9) A law enforcement chief who is a designated customs official may consider that the condition in subsection (1)(a) is satisfied only if the serious crime relates to a matter in respect of which a designated customs official has functions.

(10) A law enforcement chief who is the chair of the Competition and Markets Authority may consider that the condition in subsection (1)(a) is satisfied only if the offence, or all of the offences, to which the serious crime relates are offences under section 188 of the Enterprise Act 2002.

(11) A law enforcement chief who is the chairman, or a deputy chairman, of the Independent Police Complaints Commission may consider that the condition in subsection (1)(a) is satisfied only if the offence, or all of the offences, to which the serious crime relates are offences that are being investigated as part of an investigation by the Commission under Schedule 3 to the Police Reform Act 2002.

(12) A law enforcement chief who is the Police Investigations and Review Commissioner may consider that the condition in subsection (1)(a) is satisfied only if the offence, or all of the offences, to which the serious crime relates are offences that are being investigated under section 33A(b)(i) of the Police, Public Order and Criminal Justice (Scotland) Act 2006.

(13) For the purpose of subsection (7), an offence is an immigration or nationality offence if conduct constituting the offence—

(a) relates to the entitlement of one or more persons who are not nationals of the United Kingdom to enter, transit across, or be in, the United Kingdom (including conduct which relates to conditions or other controls on any such entitlement), or

(b) is undertaken for the purposes of or otherwise in relation to—

(i) the British Nationality Act 1981;

(ii) the Hong Kong Act 1985;

(iii) the Hong Kong (War Wives and Widows) Act 1996;

(iv) the British Nationality (Hong Kong) Act 1997;

(v) the British Overseas Territories Act 2002;

(vi) an instrument made under any of those Acts.

(14) In this section—

"designated customs official" has the same meaning as in Part 1 of the Borders, Citizenship and Immigration Act 2009 (see section 14(6) of that Act);

"immigration officer" means a person appointed as an immigration officer under paragraph 1 of Schedule 2 to the Immigration Act 1971.

107 Restriction on issue of warrants to certain law enforcement officers

(1) A law enforcement chief specified in subsection (2) may not issue a targeted equipment interference warrant under section 106 unless the law enforcement chief considers that there is a British Islands connection.

(2) The law enforcement chiefs specified in this subsection are—

(a) the Chief Constable of a police force maintained under section 2 of the Police Act 1996;

(b) the Commissioner, or an Assistant Commissioner, of the metropolitan police force;

(c) the Commissioner of Police for the City of London;

(d) the chief constable of the Police Service of Scotland;

(e) the Chief Constable or a Deputy Chief Constable of the Police Service of Northern Ireland;

(f) the Chief Constable of the British Transport Police Force;

(g) the Chief Constable of the Ministry for Defence Police;

(h) the chairman, or a deputy chairman, of the Independent Police Complaints Commission;

(i) the Police Investigations and Review Commissioner.

(3) The Director General of the National Crime Agency may not issue a targeted equipment interference warrant on the application of a member of a collaborative police force unless the Director General considers that there is a British Islands connection.

"Collaborative police force" has the meaning given by paragraph 2 of Part 3 of Schedule 6.

(4) For the purpose of this section, there is a British Islands connection if—

(a) any of the conduct authorised by the warrant would take place in the British Islands (regardless of the location of the equipment that would, or may, be interfered with),

(b) any of the equipment which would, or may, be interfered with would, or may, be in the British Islands at some time while the interference is taking place, or

(c) a purpose of the interference is to obtain—

(i) communications sent by, or to, a person who is, or whom the law enforcement officer believes to be, for the time being in the British Islands,

(ii) information relating to an individual who is, or whom the law enforcement officer believes to be, for the time being in the British Islands, or

(iii) equipment data which forms part of, or is connected with, communications or information falling within sub-paragraph (i) or (ii).

(5) Except as provided by subsections (1) to (3), a targeted equipment interference warrant may be issued under section 106 whether or not the person who has power to issue the warrant considers that there is a British Islands connection.

Approval of warrants by Judicial Commissioners

108 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a person's decision to issue a warrant under this Part, a Judicial Commissioner must review the person's conclusions as to the following matters—

(a) whether the warrant is necessary on any relevant grounds (see subsection (3)), and

(b) whether the conduct which would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) In subsection (1)(a), "relevant grounds" means—

(a) in the case of a decision to issue a warrant under section 102, grounds falling within section 102(5);

(b) in the case of a decision to issue a warrant under section 103, the purpose of preventing or detecting serious crime;

(c) in the case of a decision to issue a warrant under section 104, the interests of national security;

(d) in the case of a decision to issue a warrant under section 106(1), the purpose mentioned in section 106(1)(a);

(e) in the case of a decision to issue a warrant under section 106(3), the purpose mentioned in section 106(3)(a).

(4) Where a Judicial Commissioner refuses to approve a person's decision to issue a warrant under this Part, the Judicial Commissioner must give the person written reasons for the refusal.

(5) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a person's decision to issue a warrant under this Part, the person may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

109 Approval of warrants issued in urgent cases

(1) This section applies where—

(a) a warrant under this Part is issued without the approval of a Judicial Commissioner, and

(b) the person who issued the warrant considered that there was an urgent need to issue it.

(2) The person who issued the warrant must inform a Judicial Commissioner that it has been issued.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to issue the warrant, and

(b) notify the person of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the warrant was issued.

(4) If a Judicial Commissioner refuses to approve the decision to issue a warrant, the warrant—

(a) ceases to have effect (unless already cancelled), and

(b) may not be renewed,

and section 108(5) does not apply in relation to the refusal to approve the decision.

(5) Section 110 contains further provision about what happens if a Judicial Commissioner refuses to approve the decision to issue a warrant.

110 Failure to approve warrant issued in urgent case

(1) This section applies where under section 109(3) a Judicial Commissioner refuses to approve the decision to issue a warrant.

(2) The person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(3) Where the refusal relates to a targeted equipment interference warrant, the Judicial Commissioner may—

(a) authorise further interference with equipment for the purpose of enabling the person to whom the warrant was addressed to secure that anything in the process of being done under the warrant stops as soon as possible;

(b) direct that any of the material obtained under the warrant is destroyed;

(c) impose conditions as to the use or retention of any of that material.

(4) Where the refusal relates to a targeted examination warrant, the Judicial Commissioner may impose conditions as to the use of any protected material selected for examination under the warrant.

(5) The Judicial Commissioner—

(a) may require an affected party to make representations about how the Judicial Commissioner should exercise any function under subsection (3) or (4), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(6) Each of the following is an "affected party" for the purposes of subsection (5)—

(a) the person who decided to issue the warrant;

(b) the person to whom the warrant was addressed.

(7) The person who decided to issue the warrant may ask the Investigatory Powers Commissioner to review a decision made by any other Judicial Commissioner under subsection (3) or (4).

(8) On a review under subsection (7), the Investigatory Powers Commissioner may—

(a) confirm the Judicial Commissioner's decision, or

(b) make a fresh determination.

(9) Nothing in this section or section 109 affects the lawfulness of—

(a) anything done under the warrant before it ceases to have effect;

(b) if anything is in the process of being done under the warrant when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done that it is not reasonably practicable to stop.

Additional safeguards

111 Members of Parliament etc.

(1) Subsection (3) applies where—

(a) an application is made to the Secretary of State for a targeted equipment interference warrant, and

(b) the purpose of the warrant is to obtain—

(i) communications sent by, or intended for, a person who is a member of a relevant legislature, or

(ii) a member of a relevant legislature's private information.

(2) Subsection (3) also applies where—

(a) an application is made to the Secretary of State for a targeted examination warrant, and

(b) the purpose of the warrant is to authorise the selection for examination of protected material which consists of—

(i) communications sent by, or intended for, a person who is a member of a relevant legislature, or

(ii) a member of a relevant legislature's private information.

(3) The Secretary of State may not issue the warrant without the approval of the Prime Minister.

(4) Subsection (5) applies where—

(a) an application is made under section 106 to a law enforcement chief for a targeted equipment interference warrant, and

(b) the purpose of the warrant is to obtain—

(i) communications sent by, or intended for, a person who is a member of a relevant legislature, or

(ii) a member of a relevant legislature's private information.

(5) The law enforcement chief may not issue the warrant without the approval of the Secretary of State unless the law enforcement chief believes that the warrant (if issued) would authorise interference only with equipment which would be in Scotland at the time of the issue of the warrant or which the law enforcement chief believes would be in Scotland at that time.

(6) The Secretary of State may give approval for the purposes of subsection (5) only with the approval of the Prime Minister.

(7) In a case where the decision whether to issue a targeted equipment interference warrant is to be taken by an appropriate delegate in relation to a law enforcement chief under section 106(4), the reference in subsection (5) to the law enforcement chief is to be read as a reference to the appropriate delegate.

(8) In this section "member of a relevant legislature" means—

(a) a member of either House of Parliament;

(b) a member of the Scottish Parliament;

(c) a member of the National Assembly for Wales;

(d) a member of the Northern Ireland Assembly;

(e) a member of the European Parliament elected for the United Kingdom.

112 Items subject to legal privilege

(1) Subsections (2) to (5) apply if—

(a) an application is made for a warrant under this Part, and

(b) the purpose, or one of the purposes, of the warrant is—

(i) in the case of a targeted equipment interference warrant, to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege, or

(ii) in the case of a targeted examination warrant, to authorise the selection of such items for examination.

(2) The application must contain a statement that the purpose, or one of the purposes, of the warrant is to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege or (in the case of a targeted examination warrant) the selection for examination of items subject to legal privilege.

(3) In deciding whether to issue the warrant, the person to whom the application is made must have regard to the public interest in the confidentiality of items subject to legal privilege.

(4) The person to whom the application is made may issue the warrant only if the person considers—

(a) that there are exceptional and compelling circumstances which make it necessary to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege or (in the case of a targeted examination warrant) the selection for examination of items subject to legal privilege, and

(b) that the arrangements made for the purposes of section 129 or (as the case may be) section 191 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of such items.

(5) But the warrant may not be issued if it is considered necessary only as mentioned in section 102(5)(c).

(6) For the purposes of subsection (4)(a), there cannot be exceptional and compelling circumstances that make it necessary to authorise or require interference with equipment for the purpose of obtaining, or the selection for examination of, items subject to legal privilege unless—

(a) the public interest in obtaining the information that would be obtained by the warrant outweighs the public interest in the confidentiality of items subject to legal privilege,

(b) there are no other means by which the information may reasonably be obtained, and

(c) in the case of a warrant considered necessary for the purposes of preventing or detecting serious crime or as mentioned in section 106(3)(a), obtaining the information is necessary for the purpose of preventing death or significant injury.

(7) Subsections (8) and (9) apply if—

(a) an application is made for a warrant under this Part,

(b) the applicant considers that the relevant material is likely to include items subject to legal privilege, and

(c) subsections (2) to (5) do not apply.

(8) The application must contain—

(a) a statement that the applicant considers that the relevant material is likely to include items subject to legal privilege, and

(b) an assessment of how likely it is that the relevant material will include such items.

(9) The person to whom the application is made may issue the warrant only if the person considers that the arrangements made for the purposes of section 129 or (as the case may be) section 191 include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege.

(10) In this section, "relevant material" means—

(a) in relation to a targeted equipment interference warrant, any material the obtaining of which is authorised or required under the warrant;

(b) in relation to a targeted examination warrant, any protected material which the warrant authorises to be selected for examination.

(11) Subsections (12) and (13) apply if—

(a) an application is made for a warrant under this Part,

(b) the purpose, or one of the purposes, of the warrant is—

(i) in the case of a targeted equipment interference warrant, to authorise or require interference with equipment for the purpose of obtaining communications or other items of information that, if they were not communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose, would be items subject to legal privilege, or

(ii) in the case of a targeted examination warrant, to authorise the selection of such communications or other items of information for examination, and

(c) the applicant considers that the communications or the other items of information ("the targeted communications or other items of information") are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

(12) The application must—

(a) contain a statement that the purpose, or one of the purposes, of the warrant is—

(i) to authorise or require interference with equipment for the purpose of obtaining communications or other items of information that, if they were not communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose, would be items subject to legal privilege, or

(ii) (in the case of a targeted examination warrant) to authorise the selection of such communications or other items of information for examination, and

(b) set out the reasons for believing that the targeted communications or other items of information are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

(13) The person to whom the application is made may issue the warrant only if the person considers that the targeted communications or other items of information are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

113 Confidential journalistic material

(1) This section applies if an application is made for a warrant under this Part and the purpose, or one of the purposes, of the warrant—

(a) in the case of a targeted equipment interference warrant, to authorise or require interference with equipment for the purpose of obtaining communications or other items of information which the applicant for the warrant believes will be communications or other items of information containing confidential journalistic material, or

(b) in the case of a targeted examination warrant, to authorise the selection for examination of journalistic material which the applicant for the warrant believes is confidential journalistic material.

(2) The application must contain a statement that the purpose, or one of the purposes, of the warrant is—

(a) in the case of a targeted equipment interference warrant, to authorise or require interference with equipment for the purpose of obtaining communications or other items of information which the applicant for the warrant believes will be communications or other items of information containing confidential journalistic material, or

(b) in the case of a targeted examination warrant, to authorise the selection for examination of journalistic material which the applicant for the warrant believes is confidential journalistic material.

(3) The person to whom the application is made may issue the warrant only if the person considers that the arrangements made for the purposes of section 129 or (as the case may be) section 191 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of communications or other items of information containing confidential journalistic material.

(4) For the meaning of "journalistic material" and "confidential journalistic material", see section 264.

114 Sources of journalistic information

(1) This section applies if an application is made for a warrant under this Part and the purpose, or one of the purposes, of the warrant is to identify or confirm a source of journalistic information.

(For the meaning of "source of journalistic information", see section 263(1).)

(2) The application must contain a statement that the purpose, or one of the purposes, of the warrant is to identify or confirm a source of journalistic information.

(3) The person to whom the application is made may issue the warrant only if the person considers that the arrangements made for the purposes of section 129 or (as the case may be) section 191 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of communications or other items of information that identify sources of journalistic information.

Further provision about warrants

115 Requirements that must be met by warrants

(1) A warrant under this Part must contain a provision stating whether it is a targeted equipment interference warrant or a targeted examination warrant.

(2) A warrant under this Part must be addressed—

(a) in the case of a warrant issued under section 102 or 103, to the head of the intelligence service by whom or on whose behalf the application for the warrant was made;

(b) in the case of a warrant issued under section 104, to the Chief of Defence Intelligence;

(c) in the case of a warrant issued under section 106 by a law enforcement chief (or by an appropriate delegate in relation to a law enforcement chief), to a person who—

(i) is an appropriate law enforcement officer in relation to the law enforcement chief, and

(ii) is named or described in the warrant.

(3) In the case of a targeted equipment interference warrant which relates to a matter described in the first column of the Table below, the warrant must include the details specified in the second column.

Matter	*Details to be included in the warrant*
Equipment belonging to, used by or in the possession of a particular person or organisation	The name of the person or organisation or a description of the person or organisation
Equipment belonging to, used by or in the possession of persons who form a group which shares a common purpose or who carry on, or may carry on, a particular activity	A description of the purpose or activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe
Equipment used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and the name of, or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe
Equipment in a particular location	A description of the location
Equipment in more than one location, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and a description of as many of the locations as it is reasonably practicable to describe
Equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description	A description of the particular activity or activities
Equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment	A description of the nature of the testing, maintenance or development of capabilities
Equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, interference with equipment	A description of the nature of the training

(4) A targeted equipment interference warrant must also describe—

(a) the type of equipment which is to be interfered with, and

(b) the conduct which the person to whom the warrant is addressed is authorised to take.

(5) In the case of a targeted examination warrant which relates to a matter described in the first column of the Table below, the warrant must include the details specified in the second column.

Matter	*Details to be included in the warrant*
A particular person or organisation	The name of the person or organisation or a description of the person or organisation
A group of persons who share a common purpose or who carry on or may carry on a particular activity	A description of the purpose or activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe
More than one person or organisation, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and the name of, or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe
The testing, maintenance or development of capabilities relating to the selection of protected material for examination	A description of the nature of the testing, maintenance or development of capabilities
The training of persons who carry out, or are likely to carry out, the selection of protected material for examination	A description of the nature of the training

116 Duration of warrants

(1) A warrant issued under this Part ceases to have effect at the end of the relevant period (see subsection (2)), unless—

(a) it is renewed before the end of that period (see section 117), or

(b) it is cancelled or otherwise ceases to have effect before the end of that period (see sections 109 and 125).

(2) In this section, "the relevant period"—

(a) in the case of an urgent warrant which has not been renewed, means the period ending with the fifth working day after the day on which the warrant was issued;

(b) in any other case, means the period of 6 months beginning with—

(i) the day on which the warrant was issued, or

(ii) in the case of a warrant which has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) For the purposes of subsection (2)(a), a warrant is an "urgent warrant" if—

(a) the warrant was issued without the approval of a Judicial Commissioner, and

(b) the person who decided to issue the warrant considered that there was an urgent need to issue it.

117 Renewal of warrants

(1) If the renewal conditions are met, a warrant issued under this Part may be renewed, at any time during the renewal period, by an instrument issued by the appropriate person (see subsection (3)).

(2) The renewal conditions are—

(a) that the appropriate person considers that the warrant continues to be necessary on any relevant grounds,

(b) that the appropriate person considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,

(c) that, in the case of a targeted examination warrant, the appropriate person considers that the warrant continues to be necessary to authorise the selection of protected material for examination in breach of the prohibition in section 193(4), and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) The appropriate person is—

(a) in the case of a warrant issued under section 102 or 104, the Secretary of State;

(b) in the case of a warrant issued under section 103, a member of the Scottish Government;

(c) in the case of a warrant issued under section 106 by a law enforcement chief or by an appropriate delegate in relation to the law enforcement chief, either—

(i) the law enforcement chief, or

(ii) if the warrant was issued by an appropriate delegate, that person.

(4) In subsection (2)(a), "relevant grounds" means—

(a) in the case of a warrant issued under section 102, grounds falling within section 102(5),

(b) in the case of a warrant issued under section 103, the purpose of preventing or detecting serious crime,

(c) in the case of a warrant issued under section 104, the interests of national security,

(d) in the case of a warrant issued under section 106(1), the purpose mentioned in section 106(1)(a), or

(e) in the case of a warrant issued under section 106(3), the purpose mentioned in section 106(3)(a).

(5) "The renewal period" means—

(a) in the case of an urgent warrant which has not been renewed, the relevant period;

(b) in any other case, the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect.

(6) The decision to renew a warrant issued under section 102 or 104 must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(7) The decision to renew a warrant issued under section 103 must be taken personally by a member of the Scottish Government, and the instrument renewing the warrant must be signed by the person who took that decision.

(8) The instrument renewing a warrant issued under section 106 must be signed by the person who renews it.

(9) Section 108 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a warrant under this Part as it applies in relation to a decision to issue such a warrant (and accordingly any reference in that section to the person who decided to issue the warrant is to be read as a reference to the person who decided to renew it).

(10) Sections 111 to 114 (additional safeguards) apply in relation to a decision to renew a warrant under this Part as they apply in relation to a decision to issue such a warrant.

(11) In this section—

"relevant period" has the same meaning as in section 116;

"urgent warrant" is to be read in accordance with subsection (3) of that section.

118 Modification of warrants issued by the Secretary of State or Scottish Ministers

(1) The provisions of a warrant issued under section 102, 103 or 104 may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications which may be made under this section are—

(a) adding to the matters to which the warrant relates (see section 101(1) and (2)), by including the details required in relation to that matter by section 115(3) or (5);

(b) removing a matter to which the warrant relates;

(c) adding (in relation to a matter to which the warrant relates) a name or description to the names or descriptions included in the warrant in accordance with section 115(3) or (5);

(d) varying or removing (in relation to a matter to which the warrant relates) a name or description included in the warrant in accordance with section 115(3) or (5);

(e) adding to the descriptions of types of equipment included in the warrant in accordance with section 115(4)(a);

(f) varying or removing a description of a type of equipment included in the warrant in accordance with section 115(4)(a).

(3) But—

(a) where a targeted equipment interference warrant relates only to a matter specified in section 101(1)(a), only to a matter specified in section 101(1)(d), or only to both such matters, the details included in the warrant in accordance with section 115(3) may not be modified;

(b) where a targeted examination warrant relates only to a matter specified in section 101(2)(a), the details included in the warrant in accordance with section 115(5) may not be modified.

(4) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

This is subject to section 120(7).

(5) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it.

(6) Sections 119 to 122 contain further provision about making modifications under this section.

119 Persons who may make modifications under section 118

(1) The persons who may make modifications under section 118 of a warrant are (subject to subsection (2))—

(a) in the case of a warrant issued by the Secretary of State under section 102 or 104—

(i) the Secretary of State, or

(ii) a senior official acting on behalf of the Secretary of State;

(b) in the case of a warrant issued by the Scottish Ministers under section 103—

(i) a member of the Scottish Government, or

(ii) a senior official acting on behalf of the Scottish Ministers.

(2) Any of the following persons may also make modifications under section 118 of a warrant, but only where the person considers that there is an urgent need to make the modification—

(a) the person to whom the warrant is addressed;

(b) a person who holds a senior position in the same public authority as the person mentioned in paragraph (a).

Section 122 contains provision about the approval of modifications made in urgent cases.

(3) Subsection (2) is subject to section 120(4) and (5) (special rules where any of sections 111 to 114 applies in relation to the making of a modification under section 118).

(4) For the purposes of subsection (2)(b), a person holds a senior position in a public authority if—

(a) in the case of any of the intelligence services—

(i) the person is a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service, or

(ii) the person holds a position in the intelligence service of equivalent seniority to such a person;

(b) in the case of the Ministry of Defence—

(i) the person is a member of the Senior Civil Service, or

(ii) the person is of or above the rank of brigadier, commodore or air commodore.

120 Further provision about modifications under section 118

(1) A modification, other than a modification removing any matter, name or description, may be made under section 118 only if the person making the modification considers—

(a) that the modification is necessary on any relevant grounds (see subsection (2)), and

(b) that the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct.

(2) In subsection (1)(a), "relevant grounds" means—

(a) in the case of a warrant issued under section 102, grounds falling within section 102(5);

(b) in the case of a warrant issued under section 103, the purpose of preventing or detecting serious crime;

(c) in the case of a warrant issued under section 104, the interests of national security.

(3) Sections 111 to 114 (additional safeguards) apply in relation to the making of a modification to a warrant under section 118, other than a modification removing any matter, name or description, as they apply in relation to the issuing of a warrant.

(4) Where section 111 applies in relation to the making of a modification—

(a) the modification must be made by the Secretary of State, and

(b) the modification has effect only if the decision to make the modification has been approved by a Judicial Commissioner.

(5) Where section 112, 113 or 114 applies in relation to the making of a modification—

(a) the modification must be made by —

(i) the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government, or

(ii) if a senior official acting on behalf of a person within sub-paragraph (i) considers that there is an urgent need to make the modification, that senior official, and

(b) except where the person making the modification considers that there is an urgent need to make it, the modification has effect only if the decision to make the modification has been approved by a Judicial Commissioner.

(6) In a case where any of sections 111 to 114 applies in relation to the making of a modification, section 108 (approval of warrants by Judicial Commissioners) applies in relation to the decision to make the modification as it applies in relation to a decision to issue a warrant, but as if—

(a) the references in subsection (1)(a) and (b) of that section to the warrant were references to the modification, and

(b) any reference to the person who decided to issue the warrant were a reference to the person who decided to make the modification.

Section 122 contains provision about the approval of modifications made in urgent cases.

(7) If, in a case where any of sections 111 to 114 applies in relation to the making of a modification, it is not reasonably practicable for the instrument making the modification to be signed by the Secretary of State or (as the case may be) a member of the Scottish Government in accordance with section 118(4), the instrument may be

signed by a senior official designated by the Secretary of State or (as the case may be) the Scottish Ministers for that purpose.

(8) In such a case, the instrument making the modification must contain a statement that—

(a) it is not reasonably practicable for the instrument to be signed by the person who took the decision to make the modification, and

(b) the Secretary of State or (as the case may be) a member of the Scottish Government has personally and expressly authorised the making of the modification.

121 Notification of modifications

(1) As soon as is reasonably practicable after a person makes a modification of a warrant under section 118, a Judicial Commissioner must be notified of the modification and the reasons for making it.

(2) But subsection (1) does not apply where—

(a) the modification is to remove any matter, name or description included in the warrant in accordance with section 115(3) to (5),

(b) the modification is made by virtue of section 119(2), or

(c) any of sections 111 to 114 applies in relation to the making of the modification.

(3) Where a modification is made by a senior official in accordance with section 119(1) or section 120(5)(a)(ii), the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the modification and the reasons for making it.

122 Approval of modifications under section 118 made in urgent cases

(1) This section applies where a person makes a modification of a warrant by virtue of section 119(2).

(2) This section also applies where—

(a) section 112, 113 or 114 applies in relation to the making of a modification under section 118,

(b) the person making the modification does so without the approval of a Judicial Commissioner, and

(c) the person considered that there was an urgent need to make the modification.

(3) The person who made the modification must inform the appropriate person that it has been made.

(4) In this section—

"the appropriate person" is—

(a) in a case falling within subsection (1), a designated senior official, and

(b) in a case falling within subsection (2), a Judicial Commissioner;

"designated senior official" means a senior official who has been designated by the Secretary of State or (in the case of warrants issued by the Scottish Ministers) the Scottish Ministers for the purposes of this section.

(5) The appropriate person must, before the end of the relevant period—

(a) decide whether to approve the decision to make the modification, and

(b) notify the person of the appropriate person's decision.

"The relevant period" means the period ending with the third working day after the day on which the modification was made.

(6) As soon as is reasonably practicable after a designated senior official makes a decision under subsection (5)—

(a) a Judicial Commissioner must be notified of—

(i) the decision, and

(ii) if the senior official has decided to approve the decision to make the modification, the modification in question, and

(b) the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the matters mentioned in paragraph (a)(i) and (ii).

(7) If the appropriate person refuses to approve the decision to make the modification—

(a) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and

(b) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant by virtue of that modification stops as soon as possible;

and, in a case falling within subsection (2) above, section 108(5) does not apply in relation to the refusal to approve the decision.

(8) In a case where the appropriate person refuses to approve a decision to make a modification of a targeted equipment interference warrant, the appropriate person may authorise further interference with equipment for the purpose of enabling the person to whom the warrant is addressed to secure that anything in the process of being done under the warrant by virtue of the modification stops as soon as possible.

(9) If the appropriate person authorises further interference with equipment under subsection (8), the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the authorisation.

(10) Nothing in this section affects the lawfulness of—

(a) anything done under the warrant by virtue of the modification before the modification ceases to have effect;

(b) if anything is in the process of being done under the warrant by virtue of the modification when the modification ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done which it is not reasonably practicable to stop.

123 Modification of warrants issued by law enforcement chiefs

(1) The provisions of a warrant issued under section 106 by a law enforcement chief, or by an appropriate delegate in relation to that chief, may be modified at any time—

(a) by the law enforcement chief, or

(b) if the warrant was issued by an appropriate delegate, by that person.

(2) The only modifications which may be made under this section are—

(a) adding to the matters to which the warrant relates (see section 101(1) and (2)), by including the details required in relation to that matter by section 115(3) or (5);

(b) removing a matter to which the warrant relates;

(c) adding (in relation to a matter to which the warrant relates) a name or description to the names or descriptions included in the warrant in accordance with section 115(3) or (5);

(d) varying or removing (in relation to a matter to which the warrant relates) a name or description included in the warrant in accordance with section 115(3) or (5);

(e) adding to the descriptions of types of equipment included in the warrant in accordance with section 115(4)(a);

(f) varying or removing a description of a type of equipment included in the warrant in accordance with section 115(4)(a).

(3) But where a warrant relates only to a matter specified in section 101(1)(a), only to a matter specified in section 101(1)(d), or only to both such matters, the details included in the warrant in accordance with section 115(3) may not be modified.

(4) A modification may be made only if—

(a) except in the case of a modification removing any matter, name or description, the person making the modification considers that—

(i) the modification is necessary on any relevant grounds (see subsection (5)), and

(ii) the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct, and

(b) except where the person making the modification considers that there is an urgent need to make it, the decision to make the modification has been approved by a Judicial Commissioner.

(5) In subsection (4)(a), "relevant grounds" means—

(a) in the case of a warrant issued under section 106(1), the purpose mentioned in section 106(1)(a);

(b) in the case of a warrant issued under section 106(3), the purpose mentioned in section 106(3)(a).

(6) The decision to make any modification must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

(7) Section 108 (approval of warrants by Judicial Commissioners) applies in relation to a decision to make a modification of a warrant issued under section 106 as it applies in relation to a decision to issue such a warrant, but as if—

(a) the references in subsection (1)(a) and (b) of that section to the warrant were references to the modification, and

(b) any reference to the person who decided to issue the warrant were a reference to the person who decided to make the modification.

(8) Sections 111 to 114 (additional safeguards) apply in relation to the making of a modification to a warrant under this section, other than a modification removing any matter, name or description, as they apply in relation to the issuing of a warrant.

(9) In the application of section 111 in accordance with subsection (8), subsection (5) is to be read as if for the words from "unless" to the end of the subsection there were substituted "unless the law enforcement chief believes that the warrant (as modified) would authorise interference only with equipment which would be in Scotland at the time of the making of the modification or which the law enforcement chief believes would be in Scotland at that time".

(10) Where section 111 applies in relation to the making of a modification to a warrant under this section, subsection (4)(b) of this section has effect in relation to the making of the modification as if the words "except where the person making the modification considers that there is an urgent need to make it" were omitted.

(11) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it.

124 Approval of modifications under section 123 in urgent cases

(1) This section applies where—

(a) a modification is made under section 123 without the approval of a Judicial Commissioner, and

(b) the person who made the modification considered that there was an urgent need to make it.

(2) The person who made the modification must inform a Judicial Commissioner that it has been made.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to make the modification, and

(b) notify the person of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the modification was made.

(4) If the Judicial Commissioner refuses to approve the decision to make the modification—

(a) the person who issued the warrant must be notified of the refusal,

(b) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and

(c) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant by virtue of that modification stops as soon as possible;

and section 108(5) does not apply in relation to the refusal to approve the decision.

(5) In a case where a Judicial Commissioner refuses to approve a decision to make a modification of a targeted equipment interference warrant, the Judicial Commissioner may authorise further interference with equipment for the purpose of enabling the person to whom the warrant is addressed to secure that anything in the process of being done under the warrant by virtue of the modification stops as soon as possible.

(6) If the Judicial Commissioner authorises further interference with equipment under subsection (5), the person who issued the warrant must be informed of the authorisation.

(7) Nothing in this section affects the lawfulness of—

(a) anything done under the warrant by virtue of the modification before the modification ceases to have effect;

(b) if anything is in the process of being done under the warrant by virtue of the modification when the modification ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done which it is not reasonably practicable to stop.

125 Cancellation of warrants

(1) Any of the appropriate persons may cancel a warrant issued under this Part at any time.

(2) If any of the appropriate persons considers that—

(a) a warrant issued under this Part is no longer necessary on any relevant grounds, or

(b) the conduct authorised by a warrant issued under this Part is no longer proportionate to what is sought to be achieved by the conduct,

the person must cancel the warrant.

(3) In subsection (2)(a), "relevant grounds" means—

(a) in the case of a warrant issued under section 102, grounds falling within section 102(5);

(b) in the case of a warrant issued under section 103, the purpose of preventing or detecting serious crime;

(c) in the case of a warrant issued under section 104, the interests of national security;

(d) in the case of a warrant issued under section 106(1), the purpose mentioned in section 106(1)(a);

(e) in the case of a warrant issued under section 106(3), the purpose mentioned in section 106(3)(a).

(4) For the purposes of this section, "the appropriate persons" are—

(a) in the case of a warrant issued by the Secretary of State under section 102 or 104, the Secretary of State or a senior official acting on behalf of the Secretary of State;

(b) in the case of a warrant issued by the Scottish Ministers under section 103, a member of the Scottish Government or a senior official acting on behalf of the Scottish Ministers;

(c) in the case of a warrant issued under section 106 by a law enforcement chief or by an appropriate delegate in relation to the law enforcement chief, either—

(i) the law enforcement chief, or

(ii) if the warrant was issued by an appropriate delegate, that person.

(5) Where a warrant is cancelled under this section, the person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(6) A warrant that has been cancelled under this section may not be renewed.

Implementation of warrants

126 Implementation of warrants

(1) In giving effect to a targeted equipment interference warrant, the person to whom it is addressed ("the implementing authority") may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under subsection (2) or otherwise) to provide the authority with assistance in giving effect to the warrant.

(2) For the purpose of requiring any person to provide assistance in relation to a targeted equipment interference warrant, the implementing authority may—

(a) serve a copy of the warrant on any person whom the implementing authority considers may be able to provide such assistance, or

(b) make arrangements for the service of a copy of the warrant on any such person.

(3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(4) For the purposes of this Act, the provision of assistance in giving effect to a targeted equipment interference warrant includes any disclosure to the implementing authority, or to persons acting on that person's behalf, of material obtained under the warrant.

(5) The references in subsections (2) and (3) and sections 127 and 128 to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in it.

127 Service of warrants

(1) This section applies to the service of warrants under section 126(2).

(2) A copy of the warrant must be served in such a way as to bring the contents of the warrant to the attention of the person who the implementing authority considers may be able to provide assistance in relation to it.

(3) A copy of a warrant may be served on a person outside the United Kingdom in any of the following ways (as well as by electronic or other means of service)—

(a) by serving it at the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, at any place in the United Kingdom where the person carries on business or conducts activities;

(b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept service of documents of the same description as a copy of a warrant, by serving it at that address;

(c) by making it available for inspection (whether to the person or to someone acting on the person's behalf) at a place in the United Kingdom (but this is subject to subsection (4)).

(4) A copy of a warrant may be served on a person outside the United Kingdom in the way mentioned in subsection (3)(c) only if—

(a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (3)(a) or (b) or otherwise), and

(b) the implementing authority takes such steps as it considers appropriate for the purpose of bringing the contents of the warrant, and the availability of a copy for inspection, to the attention of the person.

(5) The steps mentioned in subsection (4)(b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.

(6) In this section, "the implementing authority" has the same meaning as in section 126.

128 Duty of telecommunications operators to assist with implementation

(1) A telecommunications operator that has been served with a copy of a targeted equipment interference warrant issued by the Secretary of State under section 102 or 104, or by the Scottish Ministers under section 103, must take all steps for giving effect to the warrant which are notified to the telecommunications operator by or on behalf of the person to whom the warrant is addressed.

(2) A telecommunications operator that has been served with a copy of a targeted equipment interference warrant issued under section 106 and addressed to a law enforcement officer mentioned in subsection (3) must take all steps for giving effect to the warrant which—

(a) were approved by the Secretary of State or, in the case of a warrant addressed to a constable of the Police Service of Scotland, by the Scottish Ministers, before the warrant was served, and

(b) are notified to the telecommunications operator by or on behalf of the law enforcement officer.

(3) The law enforcement officers mentioned in this subsection are—

(a) a National Crime Agency officer;

(b) an officer of Revenue and Customs;

(c) a constable of the Police Service of Scotland;

(d) a member of the Police Service of Northern Ireland;

(e) a member of the metropolitan police force.

(4) The Secretary of State or the Scottish Ministers may give approval for the purposes of subsection (2)(a) if the Secretary of State or (as the case may be) the Scottish Ministers consider that—

(a) it is necessary for the telecommunications operator to be required to take the steps, and

(b) the steps are proportionate to what is sought to be achieved by them.

(5) A telecommunications operator is not required to take any steps which it is not reasonably practicable for the telecommunications operator to take.

(6) Where obligations have been imposed on a telecommunications operator ("P") under section 253 (technical capability notices), for the purposes of subsection (5) the steps which it is reasonably practicable for P to take include every step which it would have been reasonably practicable for P to take if P had complied with all of those obligations.

(7) The duty imposed by subsection (1) or (2) is enforceable against a person in the United Kingdom by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

Supplementary provision

129 Safeguards relating to retention and disclosure of material

(1) The issuing authority must ensure, in relation to every targeted equipment interference warrant issued by that authority, that arrangements are in force for securing that the requirements of subsections (2) and (5) are met in relation to the material obtained under the warrant.

This is subject to subsection (10).

(2) The requirements of this subsection are met in relation to the material obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))—

(a) the number of persons to whom any of the material is disclosed or otherwise made available;

(b) the extent to which any of the material is disclosed or otherwise made available;

(c) the extent to which any of the material is copied;

(d) the number of copies that are made.

(3) For the purposes of subsection (2), something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary on any relevant grounds (see subsection (7)),

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the person to whom the warrant is or was addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or of the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary for the purpose of legal proceedings, or

(e) it is necessary for the performance of the functions of any person under any enactment.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the material obtained under a warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any grounds for retaining a copy of any material if, and only if—

(a) its retention is not necessary, or not likely to become necessary, on any relevant grounds (see subsection (7)), and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (3) above.

(7) In subsections (3) and (6), "relevant grounds" means—

(a) in relation to a warrant issued under section 102, grounds falling within section 102(5);

(b) in relation to a warrant issued under section 103, the purpose of preventing or detecting serious crime;

(c) in relation to a warrant issued under section 104, the interests of national security;

(d) in the case of a warrant issued under section 106(1), the purpose mentioned in section 106(1)(a);

(e) in the case of a warrant issued under section 106(3), the purpose mentioned in section 106(3)(a).

(8) Where—

(a) material obtained under a targeted equipment interference warrant is retained, following its examination, for purposes other than the destruction of the material, and

(b) it is material that contains confidential journalistic material or identifies a source of journalistic material,

the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

(9) Subsection (10) applies if—

(a) any material obtained under the warrant has been handed over to any overseas authorities, or

(b) a copy of any such material has been given to any overseas authorities.

(10) To the extent that the requirements of subsections (2) and (5) relate to any of the material mentioned in subsection (9)(a), or to the copy mentioned in subsection (9)(b), the arrangements made for the purpose of this section are not required to secure that those requirements are met (see instead section 130).

(11) In this section—

"copy", in relation to material obtained under a warrant, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the material which identifies the material as having been obtained under the warrant, and

(b) any record which is a record of the identities of persons who owned, used or were in possession of the equipment which was interfered with to obtain that material,

and "copied" is to be read accordingly;

"the issuing authority" means—

(a) in the case of a warrant issued under section 102 or 104, the Secretary of State;

(b) in the case of a warrant issued under section 103, the Scottish Ministers;

(c) in the case of a warrant issued under section 106, the law enforcement chief who issued the warrant (or on whose behalf it was issued);

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

130 Safeguards relating to disclosure of material overseas

(1) The issuing authority must ensure, in relation to every targeted equipment interference warrant, that arrangements are in force for securing that—

(a) any material obtained under the warrant is handed over to overseas authorities only if the requirements of subsection (2) are met, and

(b) copies of any such material are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of a warrant if it appears to the issuing authority that requirements corresponding to the requirements of section 129(2) and (5) will apply, to such extent (if any) as the issuing authority considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question.

(3) In this section—

"copy" has the same meaning as in section 129;

"issuing authority" also has the same meaning as in that section;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

131 Additional safeguards for items subject to legal privilege

(1) This section applies where an item subject to legal privilege which has been obtained under a targeted equipment interference warrant is retained, following its examination, for purposes other than the destruction of the item.

(2) The person to whom the warrant is addressed must inform the Investigatory Powers Commissioner of the retention of the item as soon as is reasonably practicable.

(3) Unless the Investigatory Powers Commissioner considers that subsection (5) applies to the item, the Commissioner must—

(a) direct that the item is destroyed, or

(b) impose one or more conditions as to the use or retention of that item.

(4) If the Investigatory Powers Commissioner considers that subsection (5) applies to the item, the Commissioner may nevertheless impose such conditions under subsection (3)(b) as the Commissioner considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege.

(5) This subsection applies to an item subject to legal privilege if—

(a) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and

(b) retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(6) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsection (3), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(7) Each of the following is an "affected party" for the purposes of subsection (6)—

(a) the issuing authority (within the meaning given by section 129(11));

(b) the person to whom the warrant is or was addressed.

132 Duty not to make unauthorised disclosures

(1) A person to whom this section applies must not make an unauthorised disclosure to another person.

(2) A person makes an unauthorised disclosure for the purposes of this section if—

(a) the person discloses any of the matters within subsection (4) in relation to a warrant under this Part, and

(b) the disclosure is not an excepted disclosure (see section 133).

(3) This section applies to the following persons—

(a) any person who may apply for a warrant under this Part;

(b) any person holding office under the Crown;

(c) any person employed by, or for the purposes of, a police force;

(d) any telecommunications operator;

(e) any person employed or engaged for the purposes of any business of a telecommunications operator;

(f) any person to whom any of the matters within subsection (4) have been disclosed in relation to a warrant under this Part.

(4) The matters referred to in subsection (2)(a) are—

(a) the existence or contents of the warrant;

(b) the details of the issue of the warrant or of any renewal or modification of the warrant;

(c) the existence or contents of any requirement to provide assistance in giving effect to the warrant;

(d) the steps taken in pursuance of the warrant or of any such requirement;

(e) any of the material obtained under the warrant in a form which identifies it as having been obtained under a warrant under this Part.

133 Section 132: meaning of "excepted disclosure"

(1) For the purposes of section 132, a disclosure made in relation to a warrant is an excepted disclosure if it falls within any of the Heads set out in—

(a) subsection (2) (disclosures authorised by warrant etc.);

(b) subsection (3) (oversight bodies);

(c) subsection (4) (legal proceedings);

(d) subsection (6) (disclosures of a general nature).

(2) Head 1 is—

(a) a disclosure authorised by the warrant;

(b) a disclosure authorised by the person to whom the warrant is or was addressed or under any arrangements made by that person for the purposes of this section;

(c) a disclosure authorised by the terms of any requirement to provide assistance in giving effect to the warrant (including any requirement for disclosure imposed by virtue of section 126(4)).

(3) Head 2 is—

(a) a disclosure made to, or authorised by, a Judicial Commissioner;

(b) a disclosure made to the Independent Police Complaints Commission for the purposes of facilitating the carrying out of any of its functions;

(c) a disclosure made to the Intelligence and Security Committee of Parliament for the purposes of facilitating the carrying out of any of its functions.

(4) Head 3 is—

(a) a disclosure made—

(i) in contemplation of, or in connection with, any legal proceedings, and

(ii) for the purposes of those proceedings;

(b) a disclosure made—

(i) by a professional legal adviser ("L") to L's client or a representative of L's client, or

(ii) by L's client, or by a representative of L's client, to L,

in connection with the giving, by L to L's client, of advice about the effect of the provisions of this Part.

(5) But a disclosure within Head 3 is not an excepted disclosure if it is made with the intention of furthering a criminal purpose.

(6) Head 4 is—

(a) a disclosure which—

(i) is made by a telecommunications operator in accordance with a requirement imposed by regulations made by the Secretary of State, and

(ii) consists of statistical information of a description specified in the regulations;

(b) a disclosure of information that does not relate to any particular warrant under this Part but relates to such warrants in general.

134 Offence of making unauthorised disclosure

(1) A person commits an offence if—

(a) the person discloses any matter in breach of section 132(1), and

(b) the person knew that the disclosure was in breach of that section.

(2) A person who is guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine, or to both.

(3) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure.

135 Part 5: interpretation

(1) In this Part—

"communication" includes—

(a) anything comprising speech, music, sounds, visual images or data of any description, and

(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;

"equipment" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment;

"equipment data" has the meaning given by section 100;

"private information" includes information relating to a person's private or family life;

"protected material", in relation to a targeted examination warrant, has the meaning given by section 99(9);

"senior official" means—

(a) in the case of a targeted equipment interference warrant which is or may be issued by the Secretary of State or a law enforcement chief, or in the case of a targeted examination warrant which is or may be issued by the Secretary of State, a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

(b) in the case of a targeted equipment interference warrant or a targeted examination warrant which is or may be issued by the Scottish Ministers, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service;

"targeted examination warrant" has the meaning given by section 99(9).

(2) See also—

section 261 (telecommunications definitions),

section 263 (general definitions),

section 264 (general definitions: "journalistic material" etc.),
section 265 (index of defined expressions).

PART 6

BULK WARRANTS

CHAPTER 1

BULK INTERCEPTION WARRANTS

Bulk interception warrants

136 Bulk interception warrants

(1) For the purposes of this Act a "bulk interception warrant" is a warrant issued under this Chapter which meets conditions A and B.

(2) Condition A is that the main purpose of the warrant is one or more of the following—

(a) the interception of overseas-related communications (see subsection (3));

(b) the obtaining of secondary data from such communications (see section 137).

(3) In this Chapter "overseas-related communications" means—

(a) communications sent by individuals who are outside the British Islands, or

(b) communications received by individuals who are outside the British Islands.

(4) Condition B is that the warrant authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following activities—

(a) the interception, in the course of their transmission by means of a telecommunication system, of communications described in the warrant;

(b) the obtaining of secondary data from communications transmitted by means of such a system and described in the warrant;

(c) the selection for examination, in any manner described in the warrant, of intercepted content or secondary data obtained under the warrant;

(d) the disclosure, in any manner described in the warrant, of anything obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(5) A bulk interception warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including—

(i) the interception of communications not described in the warrant, and

(ii) conduct for obtaining secondary data from such communications;

(b) conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant;

(c) any conduct for obtaining related systems data from any telecommunications operator.

(6) For the purposes of subsection (5)(c)—

"related systems data", in relation to a warrant, means systems data relating to a relevant communication or to the sender or recipient, or intended recipient, of a relevant communication (whether or not a person), and

"relevant communication", in relation to a warrant, means—

(a) any communication intercepted in accordance with the warrant in the course of its transmission by means of a telecommunication system, or

(b) any communication from which secondary data is obtained under the warrant.

137 Obtaining secondary data

(1) This section has effect for the purposes of this Chapter.

(2) References to obtaining secondary data from a communication transmitted by means of a telecommunication system are references to obtaining such data—

(a) while the communication is being transmitted, or

(b) at any time when the communication is stored in or by the system (whether before or after its transmission),

and references to secondary data obtained under a bulk interception warrant are to be read accordingly.

(3) "Secondary data", in relation to a communication transmitted by means of a telecommunication system, means any data falling within subsection (4) or (5).

(4) The data falling within this subsection is systems data which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise).

(5) The data falling within this subsection is identifying data which—

(a) is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise),

(b) is capable of being logically separated from the remainder of the communication, and

(c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication.

(6) For the meaning of "systems data" and "identifying data", see section 263.

138 Power to issue bulk interception warrants

(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a bulk interception warrant if—

(a) the Secretary of State considers that the main purpose of the warrant is one or more of the following—

(i) the interception of overseas-related communications, and

(ii) the obtaining of secondary data from such communications,

(b) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within subsection (2),

(c) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) the Secretary of State considers that—

(i) each of the specified operational purposes (see section 142) is a purpose for which the examination of intercepted content or secondary data obtained under the warrant is or may be necessary, and

(ii) the examination of intercepted content or secondary data for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary,

(e) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 150 and 151 (safeguards relating to disclosure etc.) are in force in relation to the warrant,

(f) in a case where the Secretary of State considers that a telecommunications operator outside the United Kingdom is likely to be required to provide assistance in giving effect to the warrant if it is issued, the Secretary of State has complied with section 139, and

(g) the decision to issue the warrant has been approved by a Judicial Commissioner.

For the meaning of "head of an intelligence service", see section 263.

(2) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) for the purpose of preventing or detecting serious crime, or

(b) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security (but see subsection (3)).

(3) A warrant may be considered necessary on the ground falling within subsection (2)(b) only if the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.

(4) A warrant may not be considered necessary in the interests of national security or on any other grounds falling within subsection (2) if it is considered necessary only for the purpose of gathering evidence for use in any legal proceedings.

(5) An application for the issue of a bulk interception warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

139 Additional requirements in respect of warrants affecting overseas operators

(1) This section applies where—

(a) an application for a bulk interception warrant has been made, and

(b) the Secretary of State considers that a telecommunications operator outside the United Kingdom is likely to be required to provide assistance in giving effect to the warrant if it is issued.

(2) Before issuing the warrant, the Secretary of State must consult the operator.

(3) Before issuing the warrant, the Secretary of State must, among other matters, take into account—

(a) the likely benefits of the warrant,
(b) the likely number of users (if known) of any telecommunications service which is provided by the operator and to which the warrant relates,
(c) the technical feasibility of complying with any requirement that may be imposed on the operator to provide assistance in giving effect to the warrant,
(d) the likely cost of complying with any such requirement, and
(e) any other effect of the warrant on the operator.

140 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a decision to issue a warrant under section 138, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—
(a) whether the warrant is necessary as mentioned in subsection (1)(b) of that section,
(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct,
(c) whether—
(i) each of the specified operational purposes (see section 142) is a purpose for which the examination of intercepted content or secondary data obtained under the warrant is or may be necessary, and
(ii) the examination of intercepted content or secondary data for each such purpose is necessary as mentioned in section 138(1)(d)(ii), and
(d) any matters taken into account in accordance with section 139.

(2) In doing so, the Judicial Commissioner must—
(a) apply the same principles as would be applied by a court on an application for judicial review, and
(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 138, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant under section 138, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

141 Decisions to issue warrants to be taken personally by Secretary of State

(1) The decision to issue a bulk interception warrant must be taken personally by the Secretary of State.

(2) Before a bulk interception warrant is issued, it must be signed by the Secretary of State.

142 Requirements that must be met by warrants

(1) A bulk interception warrant must contain a provision stating that it is a bulk interception warrant.

(2) A bulk interception warrant must be addressed to the head of the intelligence service by whom, or on whose behalf, the application for the warrant was made.

(3) A bulk interception warrant must specify the operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination.

(4) The operational purposes specified in the warrant must be ones specified, in a list maintained by the heads of the intelligence services ("the list of operational purposes"), as purposes which they consider are operational purposes for which intercepted content or secondary data obtained under bulk interception warrants may be selected for examination.

(5) The warrant may, in particular, specify all of the operational purposes which, at the time the warrant is issued, are specified in the list of operational purposes.

(6) An operational purpose may be specified in the list of operational purposes only with the approval of the Secretary of State.

(7) The Secretary of State may give such approval only if satisfied that the operational purpose is specified in a greater level of detail than the descriptions contained in section 138(1)(b) or (2).

(8) At the end of each relevant three-month period the Secretary of State must give a copy of the list of operational purposes to the Intelligence and Security Committee of Parliament.

(9) In subsection (8) "relevant three-month period" means—

(a) the period of three months beginning with the day on which this section comes into force, and

(b) each successive period of three months.

(10) The Prime Minister must review the list of operational purposes at least once a year.

(11) In this Chapter "the specified operational purposes", in relation to a bulk interception warrant, means the operational purposes specified in the warrant in accordance with this section.

Duration, modification and cancellation of warrants

143 Duration of warrants

(1) A bulk interception warrant (unless already cancelled) ceases to have effect at the end of the period of 6 months beginning with—

(a) the day on which the warrant was issued, or

(b) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(2) For provision about the renewal of warrants, see section 144.

144 Renewal of warrants

(1) If the renewal conditions are met, a bulk interception warrant may be renewed, at any time during the renewal period, by an instrument issued by the Secretary of State.

This is subject to subsection (6).

(2) The renewal conditions are—

(a) that the Secretary of State considers that the warrant continues to be necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within section 138(2),

(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,

(c) that the Secretary of State considers that—

(i) each of the specified operational purposes (see section 142) is a purpose for which the examination of intercepted content or secondary data obtained under the warrant continues to be, or may be, necessary, and

(ii) the examination of intercepted content or secondary data for each such purpose continues to be necessary on any of the grounds on which the Secretary of State considers that the warrant continues to be necessary, and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) "The renewal period" means the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect.

(4) The decision to renew a bulk interception warrant must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(5) Section 140 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a bulk interception warrant as it applies in relation to a decision to issue a bulk interception warrant, but with the omission of paragraph (d) of subsection (1).

This is subject to subsection (6).

(6) In the case of the renewal of a bulk interception warrant that has been modified so that it no longer authorises or requires the interception of communications or the obtaining of secondary data—

(a) the renewal condition in subsection (2)(a) is to be disregarded,

(b) the reference in subsection (2)(c)(ii) to the grounds on which the Secretary of State considers the warrant to be necessary is to be read as a reference to any grounds falling within section 138(1)(b) or (2), and

(c) section 140 has effect as if—

(i) paragraph (a) of subsection (1) were omitted, and

(ii) the reference in subsection (1)(c)(ii) to the grounds on which the Secretary of State considers the warrant to be necessary were a reference to any grounds falling within section 138(1)(b) or (2).

145 Modification of warrants

(1) The provisions of a bulk interception warrant may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications that may be made under this section are—

(a) adding, varying or removing any operational purpose specified in the warrant as a purpose for which any intercepted content or secondary data obtained under the warrant may be selected for examination, and

(b) providing that the warrant no longer authorises or requires (to the extent that it did so previously)—

(i) the interception of any communications in the course of their transmission by means of a telecommunication system, or

(ii) the obtaining of any secondary data from communications transmitted by means of such a system.

(3) In this section—

(a) a modification adding or varying any operational purpose as mentioned in paragraph (a) of subsection (2) is referred to as a "major modification", and

(b) any other modification within that subsection is referred to as a "minor modification".

(4) A major modification—

(a) must be made by the Secretary of State, and

(b) may be made only if the Secretary of State considers that it is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary (see section 138(1)(b)).

(5) Except where the Secretary of State considers that there is an urgent need to make the modification, a major modification has effect only if the decision to make the modification is approved by a Judicial Commissioner.

(6) A minor modification may be made by—

(a) the Secretary of State, or

(b) a senior official acting on behalf of the Secretary of State.

(7) Where a minor modification is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

(8) If at any time a person mentioned in subsection (6) considers that any operational purpose specified in a warrant is no longer a purpose for which the examination of intercepted content or secondary data obtained under the warrant is or may be necessary, the person must modify the warrant by removing that operational purpose.

(9) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

This is subject to subsection (10).

(10) If it is not reasonably practicable for an instrument making a major modification to be signed by the Secretary of State, the instrument may be signed by a senior official designated by the Secretary of State for that purpose.

(11) In such a case, the instrument making the modification must contain a statement that—

(a) it is not reasonably practicable for the instrument to be signed by the Secretary of State, and

(b) the Secretary of State has personally and expressly authorised the making of the modification.

(12) Despite section 136(2), the modification of a bulk interception warrant as mentioned in subsection (2)(b) above does not prevent the warrant from being a bulk interception warrant.

(13) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it.

146 Approval of major modifications by Judicial Commissioners

(1) In deciding whether to approve a decision to make a major modification of a bulk interception warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to make a major modification under section 145, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to make a major modification under section 145, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to make the modification.

147 Approval of major modifications made in urgent cases

(1) This section applies where—

(a) the Secretary of State makes a major modification of a bulk interception warrant without the approval of a Judicial Commissioner, and

(b) the Secretary of State considered that there was an urgent need to make the modification.

(2) The Secretary of State must inform a Judicial Commissioner that the modification has been made.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to make the modification, and

(b) notify the Secretary of State of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the modification was made.

(4) If the Judicial Commissioner refuses to approve the decision to make the modification—

(a) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and

(b) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant by virtue of that modification stops as soon as possible,

and section 146(4) does not apply in relation to the refusal to approve the decision.

(5) Nothing in this section affects the lawfulness of—

(a) anything done under the warrant by virtue of the modification before the modification ceases to have effect;

(b) if anything is in the process of being done under the warrant by virtue of the modification when the modification ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done which it is not reasonably practicable to stop.

148 Cancellation of warrants

(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a bulk interception warrant at any time.

(2) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, considers that any of the cancellation conditions are met in relation to a bulk interception warrant, the person must cancel the warrant.

(3) The cancellation conditions are—

(a) that the warrant is no longer necessary in the interests of national security;

(b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct;

(c) that the examination of intercepted content or secondary data obtained under the warrant is no longer necessary for any of the specified operational purposes (see section 142).

(4) But the condition in subsection (3)(a) does not apply where the warrant has been modified so that it no longer authorises or requires the interception of communications or the obtaining of secondary data.

(5) Where a warrant is cancelled under this section, the person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(6) A warrant that has been cancelled under this section may not be renewed.

Implementation of warrants

149 Implementation of warrants

(1) In giving effect to a bulk interception warrant, the person to whom it is addressed ("the implementing authority") may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under

subsection (2) or otherwise) to provide the authority with assistance in giving effect to the warrant.

(2) For the purpose of requiring any person to provide assistance in relation to a bulk interception warrant, the implementing authority may—

(a) serve a copy of the warrant on any person who the implementing authority considers may be able to provide such assistance, or

(b) make arrangements for the service of a copy of the warrant on any such person.

(3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(4) For the purposes of this Act, the provision of assistance in giving effect to a bulk interception warrant includes any disclosure to the implementing authority, or to persons acting on behalf of the implementing authority, of anything obtained under the warrant.

(5) Sections 42 (service of warrants) and 43 (duty of operators to assist with implementation) apply in relation to a bulk interception warrant as they apply in relation to a targeted interception warrant.

(6) References in this section (and in sections 42 and 43 as they apply in relation to bulk interception warrants) to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in the warrant.

Restrictions on use or disclosure of material obtained under warrants etc.

150 Safeguards relating to retention and disclosure of material

(1) The Secretary of State must ensure, in relation to every bulk interception warrant, that arrangements are in force for securing—

(a) that the requirements of subsections (2) and (5) are met in relation to the material obtained under the warrant, and

(b) that the requirements of section 152 are met in relation to the intercepted content or secondary data obtained under the warrant.

This is subject to subsection (8).

(2) The requirements of this subsection are met in relation to the material obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))—

(a) the number of persons to whom any of the material is disclosed or otherwise made available;

(b) the extent to which any of the material is disclosed or otherwise made available;

(c) the extent to which any of the material is copied;

(d) the number of copies that are made.

(3) For the purposes of subsection (2) something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 138(2),

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is or was addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution, or

(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the material obtained under a warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any relevant grounds for retaining a copy of any material if, and only if—

(a) its retention is not necessary, or not likely to become necessary, in the interests of national security or on any other grounds falling within section 138(2), and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (3) above.

(7) Subsection (8) applies if—

(a) any material obtained under the warrant has been handed over to any overseas authorities, or

(b) a copy of any such material has been given to any overseas authorities.

(8) To the extent that the requirements of subsections (2) and (5) and section 152 relate to any of the material mentioned in subsection (7)(a), or to the copy mentioned in subsection (7)(b), the arrangements made for the purposes of this section are not required to secure that those requirements are met (see instead section 151).

(9) In this section—

"copy", in relation to material obtained under a warrant, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the material which identifies the material as having been obtained under the warrant, and

(b) any record which—

(i) refers to any interception or to the obtaining of any material, and

(ii) is a record of the identities of the persons to or by whom the material was sent, or to whom the material relates,

and "copied" is to be read accordingly;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

151 Safeguards relating to disclosure of material overseas

(1) The Secretary of State must ensure, in relation to every bulk interception warrant, that arrangements are in force for securing that—

(a) any material obtained under the warrant is handed over to overseas authorities only if the requirements of subsection (2) are met, and

(b) copies of any such material are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of a warrant if it appears to the Secretary of State—

(a) that requirements corresponding to the requirements of section 150(2) and (5) and section 152 will apply, to such extent (if any) as the Secretary of State considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question, and

(b) that restrictions are in force which would prevent, to such extent (if any) as the Secretary of State considers appropriate, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in a prohibited disclosure.

(3) In subsection (2)(b) "prohibited disclosure" means a disclosure which, if made in the United Kingdom, would breach the prohibition in section 56(1) (see section 156).

(4) In this section—

"copy" has the same meaning as in section 150;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

152 Safeguards relating to examination of material

(1) For the purposes of section 150 the requirements of this section are met in relation to the intercepted content and secondary data obtained under a warrant if—

(a) the selection of any of the intercepted content or secondary data for examination is carried out only for the specified purposes (see subsection (2)),

(b) the selection of any of the intercepted content or secondary data for examination is necessary and proportionate in all the circumstances, and

(c) the selection of any of the intercepted content for examination meets any of the selection conditions (see subsection (3)).

(2) The selection of intercepted content or secondary data for examination is carried out only for the specified purposes if the intercepted content or secondary data is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 142.

In this subsection "specified in the warrant" means specified in the warrant at the time of the selection of the intercepted content or secondary data for examination.

(3) The selection conditions referred to in subsection (1)(c) are—

(a) that the selection of the intercepted content for examination does not breach the prohibition in subsection (4);

(b) that the person to whom the warrant is addressed considers that the selection of the intercepted content for examination would not breach that prohibition;

(c) that the selection of the intercepted content for examination in breach of that prohibition is authorised by subsection (5);

(d) that the selection of the intercepted content for examination in breach of that prohibition is authorised by a targeted examination warrant issued under Chapter 1 of Part 2.

(4) The prohibition referred to in subsection (3)(a) is that intercepted content may not at any time be selected for examination if—

(a) any criteria used for the selection of the intercepted content for examination are referable to an individual known to be in the British Islands at that time, and

(b) the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual.

It does not matter for the purposes of this subsection whether the identity of the individual is known.

(5) The selection of intercepted content ("the relevant content") for examination is authorised by this subsection if—

(a) criteria referable to an individual have been, or are being, used for the selection of intercepted content for examination in circumstances falling within subsection (3)(a) or (b),

(b) at any time it appears to the person to whom the warrant is addressed that there has been a relevant change of circumstances in relation to the individual (see subsection (6)) which would mean that the selection of the relevant content for examination would breach the prohibition in subsection (4),

(c) since that time, a written authorisation to examine the relevant content using those criteria has been given by a senior officer, and

(d) the selection of the relevant content for examination is made before the end of the permitted period (see subsection (7)).

(6) For the purposes of subsection (5)(b) there is a relevant change of circumstances in relation to an individual if—

(a) the individual has entered the British Islands, or

(b) a belief by the person to whom the warrant is addressed that the individual was outside the British Islands was in fact mistaken.

(7) In subsection (5)—

"senior officer", in relation to a warrant addressed to the head of an intelligence service, means a member of the intelligence service who—

(a) is a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service, or

(b) holds a position in the intelligence service of equivalent seniority to such a member;

"the permitted period" means the period ending with the fifth working day after the time mentioned in subsection (5)(b).

(8) In a case where the selection of intercepted content for examination is authorised by subsection (5), the person to whom the warrant is addressed must notify the Secretary of State that the selection is being carried out.

153 Additional safeguards for items subject to legal privilege

(1) Subsection (2) applies if, in a case where intercepted content obtained under a bulk interception warrant is to be selected for examination—

(a) the selection of the intercepted content for examination meets any of the selection conditions in section 152(3)(a) to (c), and

(b) either—

(i) the purpose, or one of the purposes, of using the criteria to be used for the selection of the intercepted content for examination ("the relevant criteria") is to identify any items subject to legal privilege, or

(ii) the use of the relevant criteria is likely to identify such items.

(2) The intercepted content may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(3) In deciding whether to give an approval under subsection (2) in a case where subsection (1)(b)(i) applies, a senior official must have regard to the public interest in the confidentiality of items subject to legal privilege.

(4) A senior official may give an approval under subsection (2) only if—

(a) the official considers that the arrangements made for the purposes of section 150 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege, and

(b) where subsection (1)(b)(i) applies, the official considers that there are exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria.

(5) For the purposes of subsection (4)(b), there cannot be exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria unless—

(a) the public interest in obtaining the information that would be obtained by the selection of the intercepted content for examination outweighs the public interest in the confidentiality of items subject to legal privilege,

(b) there are no other means by which the information may reasonably be obtained, and

(c) obtaining the information is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(6) Subsection (7) applies if, in a case where intercepted content obtained under a bulk interception warrant is to be selected for examination—

(a) the selection of the intercepted content for examination meets any of the selection conditions in section 152(3)(a) to (c),

(b) the purpose, or one of the purposes, of using the criteria to be used for the selection of the intercepted content for examination ("the relevant criteria") is to identify communications that, if they were not made with the intention of furthering a criminal purpose, would be items subject to legal privilege, and

(c) the person to whom the warrant is addressed considers that the communications ("the targeted communications") are likely to be communications made with the intention of furthering a criminal purpose.

(7) The intercepted content may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(8) A senior official may give an approval under subsection (7) only if the official considers that the targeted communications are likely to be communications made with the intention of furthering a criminal purpose.

(9) Where an item subject to legal privilege which has been intercepted in accordance with a bulk interception warrant is retained following its examination, for purposes other than the destruction of the item, the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

(For provision about the grounds for retaining material obtained under a warrant, see section 150.)

(10) Unless the Investigatory Powers Commissioner considers that subsection (12) applies to the item, the Commissioner must—

(a) direct that the item is destroyed, or

(b) impose one or more conditions as to the use or retention of that item.

(11) If the Investigatory Powers Commissioner considers that subsection (12) applies to the item, the Commissioner may nevertheless impose such conditions under subsection (10)(b) as the Commissioner considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege.

(12) This subsection applies to an item subject to legal privilege if—

(a) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and

(b) retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(13) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsection (10), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(14) Each of the following is an "affected party" for the purposes of subsection (13)—

(a) the Secretary of State;

(b) the person to whom the warrant is or was addressed.

154 Additional safeguard for confidential journalistic material

Where—

(a) a communication which has been intercepted in accordance with a bulk interception warrant is retained, following its examination, for purposes other than the destruction of the communication, and

(b) it is a communication containing confidential journalistic material,

the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

(For provision about the grounds for retaining material obtained under a warrant, see section 150.)

155 Offence of breaching safeguards relating to examination of material

(1) A person commits an offence if—

(a) the person selects for examination any intercepted content or secondary data obtained under a bulk interception warrant,

(b) the person knows or believes that the selection of that intercepted content or secondary data for examination does not comply with a requirement imposed by section 152 or 153, and

(c) the person deliberately selects that intercepted content or secondary data for examination in breach of that requirement.

(2) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(3) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

156 Application of other restrictions in relation to warrants

(1) Section 56 and Schedule 3 (exclusion of matters from legal proceedings etc.) apply in relation to bulk interception warrants as they apply in relation to targeted interception warrants.

(2) Sections 57 to 59 (duty not to make unauthorised disclosures) apply in relation to bulk interception warrants as they apply in relation to targeted interception warrants, but as if the reference in section 58(2)(c) to a requirement for disclosure imposed by virtue of section 41(5) were a reference to such a requirement imposed by virtue of section 149(4).

Interpretation

157 Chapter 1: interpretation

(1) In this Chapter—

"intercepted content", in relation to a bulk interception warrant, means any content of communications intercepted by an interception authorised or required by the warrant;

"overseas-related communications" has the meaning given by section 136;

"secondary data" has the meaning given by section 137, and references to obtaining secondary data from a communication are to be read in accordance with that section;

"senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

"the specified operational purposes" has the meaning given by section 142(11).

(2) See also—

section 261 (telecommunications definitions),

section 263 (general definitions),

section 264 (general definitions: "journalistic material" etc.),

section 265 (index of defined expressions).

CHAPTER 2

BULK ACQUISITION WARRANTS

Bulk acquisition warrants

158 Power to issue bulk acquisition warrants

(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a bulk acquisition warrant if—

(a) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within subsection (2),

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that—

(i) each of the specified operational purposes (see section 161) is a purpose for which the examination of communications data obtained under the warrant is or may be necessary, and

(ii) the examination of such data for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary,

(d) the Secretary of State considers that satisfactory arrangements made for the purposes of section 171 (safeguards relating to the retention and disclosure of data) are in force in relation to the warrant, and

(e) the decision to issue the warrant has been approved by a Judicial Commissioner.

For the meaning of "head of an intelligence service", see section 263.

(2) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) for the purpose of preventing or detecting serious crime, or

(b) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security (but see subsection (3)).

(3) A warrant may be considered necessary on the ground falling within subsection (2)(b) only if the communications data which it is considered necessary to obtain is communications data relating to the acts or intentions of persons outside the British Islands.

(4) The fact that the communications data which would be obtained under a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary in the interests of national security or on that ground and a ground falling within subsection (2).

(5) A bulk acquisition warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the activities in subsection (6).

(6) The activities are—

(a) requiring a telecommunications operator specified in the warrant—

(i) to disclose to a person specified in the warrant any communications data which is specified in the warrant and is in the possession of the operator,

(ii) to obtain any communications data specified in the warrant which is not in the possession of the operator but which the operator is capable of obtaining, or

(iii) to disclose to a person specified in the warrant any data obtained as mentioned in sub-paragraph (ii),

(b) the selection for examination, in any manner described in the warrant, of communications data obtained under the warrant,

(c) the disclosure, in any manner described in the warrant, of communications data obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(7) A bulk acquisition warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, and

(b) conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant.

(8) A bulk acquisition warrant may relate to data whether or not in existence at the time of the issuing of the warrant.

(9) An application for the issue of a bulk acquisition warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

159 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a decision to issue a warrant under section 158, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the warrant is necessary as mentioned in subsection (1)(a) of that section,

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, and

(c) whether—

(i) each of the specified operational purposes (see section 161) is a purpose for which the examination of communications data obtained under the warrant is or may be necessary, and

(ii) the examination of such data for each such purpose is necessary as mentioned in section 158(1)(c)(ii).

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 158, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant under section 158, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

160 Decisions to issue warrants to be taken personally by Secretary of State

(1) The decision to issue a bulk acquisition warrant must be taken personally by the Secretary of State.

(2) Before a bulk acquisition warrant is issued, it must be signed by the Secretary of State.

161 Requirements that must be met by warrants

(1) A bulk acquisition warrant must contain a provision stating that it is a bulk acquisition warrant.

(2) A bulk acquisition warrant must be addressed to the head of the intelligence service by whom, or on whose behalf, the application for the warrant was made.

(3) A bulk acquisition warrant must specify the operational purposes for which any communications data obtained under the warrant may be selected for examination.

(4) The operational purposes specified in the warrant must be ones specified, in a list maintained by the heads of the intelligence services ("the list of operational purposes"), as purposes which they consider are operational purposes for which

communications data obtained under bulk acquisition warrants may be selected for examination.

(5) The warrant may, in particular, specify all of the operational purposes which, at the time the warrant is issued, are specified in the list of operational purposes.

(6) An operational purpose may be specified in the list of operational purposes only with the approval of the Secretary of State.

(7) The Secretary of State may give such approval only if satisfied that the operational purpose is specified in a greater level of detail than the descriptions contained in section 158(1)(a) or (2).

(8) At the end of each relevant three-month period the Secretary of State must give a copy of the list of operational purposes to the Intelligence and Security Committee of Parliament.

(9) In subsection (8) "relevant three-month period" means—

(a) the period of three months beginning with the day on which this section comes into force, and

(b) each successive period of three months.

(10) The Prime Minister must review the list of operational purposes at least once a year.

(11) In this Chapter "the specified operational purposes", in relation to a bulk acquisition warrant, means the operational purposes specified in the warrant in accordance with this section.

Duration, modification and cancellation of warrants

162 Duration of warrants

(1) A bulk acquisition warrant (unless already cancelled) ceases to have effect at the end of the period of 6 months beginning with—

(a) the day on which the warrant was issued, or

(b) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(2) For provision about the renewal of warrants, see section 163.

163 Renewal of warrants

(1) If the renewal conditions are met, a bulk acquisition warrant may be renewed, at any time during the renewal period, by an instrument issued by the Secretary of State.

This is subject to subsection (6).

(2) The renewal conditions are—

(a) that the Secretary of State considers that the warrant continues to be necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within section 158(2),

(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,

(c) that the Secretary of State considers that—

(i) each of the specified operational purposes (see section 161) is a purpose for which the examination of communications data obtained under the warrant continues to be, or may be, necessary, and

(ii) the examination of such data for each such purpose continues to be necessary on any of the grounds on which the Secretary of State considers that the warrant continues to be necessary, and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) "The renewal period" means the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect.

(4) The decision to renew a bulk acquisition warrant must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(5) Section 159 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a bulk acquisition warrant as it applies in relation to a decision to issue a bulk acquisition warrant.

This is subject to subsection (6).

(6) In the case of the renewal of a bulk acquisition warrant that has been modified so that it no longer authorises or requires the carrying out of activities falling within section 158(6)(a)—

(a) the renewal condition in subsection (2)(a) is to be disregarded,

(b) the reference in subsection (2)(c)(ii) to the grounds on which the Secretary of State considers the warrant to be necessary is to be read as a reference to any grounds falling within section 158(1)(a) or (2), and

(c) section 159 has effect as if—

(i) paragraph (a) of subsection (1) were omitted, and

(ii) the reference in subsection (1)(c)(ii) to the grounds on which the Secretary of State considers the warrant to be necessary were a reference to any grounds falling within section 158(1)(a) or (2).

164 Modification of warrants

(1) The provisions of a bulk acquisition warrant may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications that may be made under this section are—

(a) adding, varying or removing any operational purpose specified in the warrant as a purpose for which any communications data obtained under the warrant may be selected for examination, and

(b) providing that the warrant no longer authorises or requires the carrying out of activities falling within section 158(6)(a).

(3) In this section—

(a) a modification adding or varying any operational purpose as mentioned in paragraph (a) of subsection (2) is referred to as a "major modification", and

(b) any other modification within that subsection is referred to as a "minor modification".

(4) A major modification—

(a) must be made by the Secretary of State, and

(b) may be made only if the Secretary of State considers that it is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary (see section 158(1)(a)).

(5) Except where the Secretary of State considers that there is an urgent need to make the modification, a major modification has effect only if the decision to make the modification is approved by a Judicial Commissioner.

(6) A minor modification may be made by—

(a) the Secretary of State, or

(b) a senior official acting on behalf of the Secretary of State.

(7) Where a minor modification is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

(8) If at any time a person mentioned in subsection (6) considers that any operational purpose specified in a warrant is no longer a purpose for which the examination of communications data obtained under the warrant is or may be necessary, the person must modify the warrant by removing that operational purpose.

(9) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

This is subject to subsection (10).

(10) If it is not reasonably practicable for an instrument making a major modification to be signed by the Secretary of State, the instrument may be signed by a senior official designated by the Secretary of State for that purpose.

(11) In such a case, the instrument making the modification must contain a statement that—

(a) it is not reasonably practicable for the instrument to be signed by the Secretary of State, and

(b) the Secretary of State has personally and expressly authorised the making of the modification.

(12) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it.

165 Approval of major modifications by Judicial Commissioners

(1) In deciding whether to approve a decision to make a major modification of a bulk acquisition warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to make a major modification under section 164, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to make a major modification under section 164, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to make the modification.

166 Approval of major modifications made in urgent cases

(1) This section applies where—

(a) the Secretary of State makes a major modification of a bulk acquisition warrant without the approval of a Judicial Commissioner, and

(b) the Secretary of State considered that there was an urgent need to make the modification.

(2) The Secretary of State must inform a Judicial Commissioner that the modification has been made.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to make the modification, and

(b) notify the Secretary of State of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the modification was made.

(4) If the Judicial Commissioner refuses to approve the decision to make the modification—

(a) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and

(b) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant by virtue of that modification stops as soon as possible,

and section 165(4) does not apply in relation to the refusal to approve the decision.

(5) Nothing in this section affects the lawfulness of—

(a) anything done under the warrant by virtue of the modification before the modification ceases to have effect,

(b) if anything is in the process of being done under the warrant by virtue of the modification when the modification ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done which it is not reasonably practicable to stop.

167 Cancellation of warrants

(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a bulk acquisition warrant at any time.

(2) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, considers that any of the cancellation conditions are met in relation to a bulk acquisition warrant, the person must cancel the warrant.

(3) The cancellation conditions are—

(a) that the warrant is no longer necessary in the interests of national security,

(b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct,

(c) that the examination of communications data obtained under the warrant is no longer necessary for any of the specified operational purposes (see section 161).

(4) But the condition in subsection (3)(a) does not apply where the warrant has been modified so that it no longer authorises or requires the carrying out of activities falling within section 158(6)(a).

(5) Where a warrant is cancelled under this section, the person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(6) A warrant that has been cancelled under this section may not be renewed.

Implementation of warrants

168 Implementation of warrants

(1) In giving effect to a bulk acquisition warrant, the person to whom it is addressed ("the implementing authority") may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under subsection (2) or otherwise) to provide the authority with assistance in giving effect to the warrant.

(2) For the purpose of requiring any person to provide assistance in relation to a bulk acquisition warrant, the implementing authority may—

(a) serve a copy of the warrant on any person whom the implementing authority considers may be able to provide such assistance, or

(b) make arrangements for the service of a copy of the warrant on any such person.

(3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(4) For the purposes of this Act, the provision of assistance in giving effect to a bulk acquisition warrant includes any disclosure to the implementing authority, or to persons acting on behalf of the implementing authority, of communications data as authorised or required under the warrant.

(5) References in this section and in sections 169 and 170 to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in the warrant.

169 Service of warrants

(1) This section applies to the service of bulk acquisition warrants under section 168(2).

(2) A copy of the warrant must be served in such a way as to bring the contents of the warrant to the attention of the person whom the implementing authority considers may be able to provide assistance in relation to it.

(3) A copy of a warrant may be served on a person outside the United Kingdom in any of the following ways (as well as by electronic or other means of service)—

(a) by serving it at the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, at any place in the United Kingdom where the person carries on business or conducts activities;

(b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept service of documents of the same description as a copy of a warrant, by serving it at that address;

(c) by making it available for inspection (whether to the person or to someone acting on the person's behalf) at a place in the United Kingdom (but this is subject to subsection (4)).

(4) A copy of a warrant may be served on a person outside the United Kingdom in the way mentioned in subsection (3)(c) only if—

(a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (3)(a) or (b) or otherwise), and

(b) the implementing authority takes such steps as the authority considers appropriate for the purpose of bringing the contents of the warrant, and the availability of a copy for inspection, to the attention of the person.

(5) The steps mentioned in subsection (4)(b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.

(6) In this section "the implementing authority" has the same meaning as in section 168.

170 Duty of operators to assist with implementation

(1) A telecommunications operator that has been served with a copy of a bulk acquisition warrant by (or on behalf of) the implementing authority must take all steps for giving effect to the warrant that are notified to the operator by (or on behalf of) the implementing authority.

This is subject to subsection (3).

(2) Subsection (1) applies whether or not the operator is in the United Kingdom.

(3) The operator is not required to take any steps which it is not reasonably practicable for the operator to take.

(4) Where obligations have been imposed on a telecommunications operator ("P") under section 253 (technical capability notices), for the purposes of subsection (3) the steps which it is reasonably practicable for P to take include every step which it would have been reasonably practicable for P to take if P had complied with all of those obligations.

(5) The duty imposed by subsection (1) is enforceable against a person in the United Kingdom by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

(6) In this section "the implementing authority" has the same meaning as in section 168.

Restrictions on use or disclosure of data obtained under warrants etc.

171 Safeguards relating to the retention and disclosure of data

(1) The Secretary of State must ensure, in relation to every bulk acquisition warrant, that arrangements are in force for securing—

(a) that the requirements of subsections (2) and (5) are met in relation to the communications data obtained under the warrant, and

(b) that the requirements of section 172 are met in relation to that data.

This is subject to subsection (8).

(2) The requirements of this subsection are met in relation to the communications data obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))—

(a) the number of persons to whom any of the data is disclosed or otherwise made available,

(b) the extent to which any of the data is disclosed or otherwise made available,

(c) the extent to which any of the data is copied,

(d) the number of copies that are made.

(3) For the purposes of subsection (2) something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 158(2),

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is or was addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution,

(e) it is necessary for use as evidence in legal proceedings, or

(f) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

(4) The arrangements for the time being in force under subsection (1) for securing that the requirements of subsection (2) are met in relation to the communications data obtained under the warrant must include arrangements for securing that every copy made of any of that data is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the communications data obtained under a warrant if every copy made of any of that data (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any relevant grounds for retaining a copy of any data if, and only if—

(a) its retention is not necessary, or not likely to become necessary, in the interests of national security or on any other grounds falling within section 158(2), and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (f) of subsection (3) above.

(7) Subsection (8) applies if—

(a) any communications data obtained under the warrant has been handed over to any overseas authorities, or

(b) a copy of any such data has been given to any overseas authorities.

(8) To the extent that the requirements of subsections (2) and (5) and section 172 relate to any of the data mentioned in subsection (7)(a), or to the copy mentioned in subsection (7)(b), the arrangements made for the purposes of subsection (1) are not required to secure that those requirements are met.

(9) But the Secretary of State must instead ensure that arrangements are in force for securing that communications data obtained under a bulk acquisition warrant, or any copy of such data, is handed over or given to an overseas authority only if the Secretary of State considers that requirements corresponding to the requirements of subsections (2) and (5) and section 172 will apply, to such extent (if any) as the Secretary of State considers appropriate, in relation to such data or copy.

(10) In this section—

"copy", in relation to communications data obtained under a warrant, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the data which identifies the data as having been obtained under the warrant, and

(b) any record referring to the obtaining of the data which is a record of the identities of the persons to whom the data relates,

and "copied" is to be read accordingly,

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

172 Safeguards relating to examination of data

(1) For the purposes of section 171 the requirements of this section are met in relation to the communications data obtained under a warrant if—

(a) any selection of the data for examination is carried out only for the specified purposes (see subsection (2)), and

(b) the selection of any of the data for examination is necessary and proportionate in all the circumstances.

(2) The selection of communications data for examination is carried out only for the specified purposes if the data is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 161.

(3) In subsection (2) "specified in the warrant" means specified in the warrant at the time of the selection of the data for examination.

173 Offence of breaching safeguards relating to examination of data

(1) A person commits an offence if—

(a) the person selects for examination any communications data obtained under a bulk acquisition warrant,

(b) the person knows or believes that the selection of that data for examination does not comply with a requirement imposed by section 172, and

(c) the person deliberately selects that data for examination in breach of that requirement.

(2) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(3) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

Supplementary provision

174 Offence of making unauthorised disclosure

(1) It is an offence for—

(a) a telecommunications operator who is under a duty by virtue of section 170 to assist in giving effect to a bulk acquisition warrant, or

(b) any person employed or engaged for the purposes of the business of such an operator,

to disclose to any person, without reasonable excuse, the existence or contents of the warrant.

(2) For the purposes of subsection (1), it is, in particular, a reasonable excuse if the disclosure is made with the permission of the Secretary of State.

(3) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

175 Chapter 2: interpretation

(1) In this Chapter—

"communications data" does not include communications data within the meaning given by section 262(3),

"senior official" means—

(a) a member of the Senior Civil Service, or

(b) a member of the Senior Management Structure of Her Majesty's Diplomatic Service,

"the specified operational purposes" has the meaning given by section 161(11).

(2) See also—

section 261 (telecommunications definitions),

section 263 (general definitions),

section 265 (index of defined expressions).

CHAPTER 3

BULK EQUIPMENT INTERFERENCE WARRANTS

Bulk equipment interference warrants

176 Bulk equipment interference warrants: general

(1) For the purposes of this Act, a warrant is a "bulk equipment interference warrant" if—

(a) it is issued under this Chapter;

(b) it authorises or requires the person to whom it is addressed to secure interference with any equipment for the purpose of obtaining—

(i) communications (see section 198);

(ii) equipment data (see section 177);

(iii) any other information; and

(c) the main purpose of the warrant is to obtain one or more of the following—

(i) overseas-related communications;

(ii) overseas-related information;

(iii) overseas-related equipment data.

(2) In this Chapter—

"overseas-related communications" means—

(a) communications sent by individuals who are outside the British Islands, or

(b) communications received by individuals who are outside the British Islands;

"overseas-related information" means information of individuals who are outside the British Islands.

(3) For the purpose of this Chapter, equipment data is "overseas-related equipment data" if—

(a) it forms part of, or is connected with, overseas-related communications or overseas-related information;

(b) it would or may assist in establishing the existence of overseas-related communications or overseas-related information or in obtaining such communications or information;

(c) it would or may assist in developing capabilities in relation to obtaining overseas-related communications or overseas-related information.

(4) A bulk equipment interference warrant—

(a) must authorise or require the person to whom it is addressed to secure the obtaining of the communications, equipment data or other information to which the warrant relates;

(b) may also authorise or require the person to whom it is addressed to secure—

(i) the selection for examination, in any manner described in the warrant, of any material obtained under the warrant by virtue of paragraph (a);

(ii) the disclosure, in any manner described in the warrant, of any such material to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(5) A bulk equipment interference warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including conduct for securing the obtaining of communications, equipment data or other information;

(b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant.

(6) A bulk equipment interference warrant may not, by virtue of subsection (4)(a), authorise a person to engage in conduct, in relation to a communication other than a stored communication, which would (unless done with lawful authority) constitute an offence under section 3(1) (unlawful interception).

(7) Subsection (5)(a) does not authorise a person to engage in conduct which could not be expressly authorised under the warrant because of the restriction imposed by subsection (6).

(8) In subsection (6), "stored communication" means a communication stored in or by a telecommunication system (whether before or after its transmission).

(9) Any conduct which is carried out in accordance with a bulk equipment interference warrant is lawful for all purposes.

177 Meaning of "equipment data"

(1) In this Chapter, "equipment data" means—

(a) systems data;

(b) data which falls within subsection (2).

(2) The data falling within this subsection is identifying data which—

(a) is, for the purposes of a relevant system, comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) or any other item of information,

(b) is capable of being logically separated from the remainder of the communication or the item of information, and

(c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication or the item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact.

(3) In subsection (2), "relevant system" means any system on or by means of which the data is held.

(4) For the meaning of "systems data" and "identifying data", see section 263.

178 Power to issue bulk equipment interference warrants

(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a bulk equipment interference warrant if—

(a) the Secretary of State considers that the main purpose of the warrant is to obtain overseas-related communications, overseas-related information or overseas-related equipment data,

(b) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within subsection (2),

(c) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) the Secretary of State considers that—

(i) each of the specified operational purposes (see section 183) is a purpose for which the examination of material obtained under the warrant is or may be necessary, and

(ii) the examination of such material for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary,

(e) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 191 and 192 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and

(f) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

For the meaning of "head of an intelligence service", see section 263.

(2) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) for the purpose of preventing or detecting serious crime, or

(b) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security (but see subsection (3)).

(3) A warrant may be considered necessary on the ground falling within subsection (2)(b) only if the interference with equipment which would be authorised by the warrant is considered necessary for the purpose of obtaining information relating to the acts or intentions of persons outside the British Islands.

(4) An application for the issue of a bulk equipment interference warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

179 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a decision to issue a warrant under section 178, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the warrant is necessary as mentioned in subsection (1)(b) of that section,

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, and

(c) whether—

(i) each of the specified operational purposes (see section 183) is a purpose for which the examination of material obtained under the warrant is or may be necessary, and

(ii) the examination of such material for each such purpose is necessary as mentioned in section 178(1)(d)(ii).

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 178, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant under section 178, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

180 Approval of warrants issued in urgent cases

(1) This section applies where—

(a) a warrant under section 178 is issued without the approval of a Judicial Commissioner, and

(b) the Secretary of State considered that there was an urgent need to issue it.

(2) The Secretary of State must inform a Judicial Commissioner that it has been issued.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to issue the warrant, and

(b) notify the Secretary of State of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the warrant was issued.

(4) If a Judicial Commissioner refuses to approve the decision to issue a warrant, the warrant—

(a) ceases to have effect (unless already cancelled), and

(b) may not be renewed,

and section 179(4) does not apply in relation to the refusal to approve the decision.

(5) Section 181 contains further provision about what happens if a Judicial Commissioner refuses to approve a decision to issue a warrant.

181 Failure to approve warrant issued in urgent case

(1) This section applies where under section 180(3) a Judicial Commissioner refuses to approve a decision to issue a warrant.

(2) The person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(3) The Judicial Commissioner may—

(a) authorise further interference with equipment for the purpose of enabling the person to whom the warrant was addressed to secure that anything in the process of being done under the warrant stops as soon as possible;

(b) direct that any material obtained under the warrant is destroyed;

(c) impose conditions as to the use or retention of any of that material.

(4) The Judicial Commissioner—

(a) may require an affected party to make representations about how the Judicial Commissioner should exercise any function under subsection (3), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(5) Each of the following is an "affected party" for the purposes of subsection (4)—

(a) the Secretary of State;

(b) the person to whom the warrant was addressed.

(6) The Secretary of State may ask the Investigatory Powers Commissioner to review a decision made by any other Judicial Commissioner under subsection (3).

(7) On a review under subsection (6), the Investigatory Powers Commissioner may—

(a) confirm the Judicial Commissioner's decision, or

(b) make a fresh determination.

(8) Nothing in this section or section 180 affects the lawfulness of—

(a) anything done under the warrant before it ceases to have effect;

(b) if anything is in the process of being done under the warrant when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done that it is not reasonably practicable to stop.

182 Decisions to issue warrants to be taken personally by Secretary of State

(1) The decision to issue a bulk equipment interference warrant must be taken personally by the Secretary of State.

(2) Before a bulk equipment interference warrant is issued, it must be signed by the Secretary of State.

(3) If it is not reasonably practicable for a warrant to be signed by the Secretary of State, the warrant may be signed by a senior official designated by the Secretary of State for that purpose.

(4) In such a case, the warrant must contain a statement that—

(a) it is not reasonably practicable for the warrant to be signed by the Secretary of State, and

(b) the Secretary of State has personally and expressly authorised the issue of the warrant.

183 Requirements that must be met by warrants

(1) A bulk equipment interference warrant must contain a provision stating that it is a bulk equipment interference warrant.

(2) A bulk equipment interference warrant must be addressed to the head of the intelligence service by whom, or on whose behalf, the application for the warrant was made.

(3) A bulk equipment interference warrant must describe the conduct that is authorised by the warrant.

(4) A bulk equipment interference warrant must specify the operational purposes for which any material obtained under the warrant may be selected for examination.

(5) The operational purposes specified in the warrant must be ones specified, in a list maintained by the heads of the intelligence services ("the list of operational purposes"), as purposes which they consider are operational purposes for which material obtained under bulk equipment interference warrants may be selected for examination.

(6) The warrant may, in particular, specify all of the operational purposes which, at the time the warrant is issued, are specified in the list of operational purposes.

(7) An operational purpose may be specified in the list of operational purposes only with the approval of the Secretary of State.

(8) The Secretary of State may give such approval only if satisfied that the operational purpose is specified in a greater level of detail than the descriptions contained in section 178(1)(b) or (2).

(9) At the end of each relevant three-month period, the Secretary of State must give a copy of the list of operational purposes to the Intelligence and Security Committee of Parliament.

(10) In subsection (9), "relevant three-month period" means—

(a) the period of three months beginning with the day on which this section comes into force, and

(b) each successive period of three months.

(11) The Prime Minister must review the list of operational purposes at least once a year.

(12) In this Chapter, "the specified operational purposes", in relation to a bulk equipment interference warrant, means the operational purposes specified in the warrant in accordance with this section.

Duration, modification and cancellation of warrants

184 Duration of warrants

(1) A bulk equipment interference warrant ceases to have effect at the end of the relevant period (see subsection (2)), unless—

(a) it is renewed before the end of that period (see section 185), or

(b) it is cancelled or otherwise ceases to have effect before the end of that period (see sections 180 and 189).

(2) In this section, "the relevant period"—

(a) in the case of an urgent warrant (see subsection (3)), means the period ending with the fifth working day after the day on which the warrant was issued;

(b) in any other case, means the period of 6 months beginning with—

(i) the day on which the warrant was issued, or

(ii) in the case of a warrant which has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) For the purposes of subsection (2)(a), a warrant is an "urgent warrant" if—

(a) the warrant was issued without the approval of a Judicial Commissioner, and

(b) the person who decided to issue the warrant considered that there was an urgent need to issue it.

185 Renewal of warrants

(1) If the renewal conditions are met, a bulk equipment interference warrant may be renewed, at any time during the renewal period, by an instrument issued by the Secretary of State.

This is subject to subsection (6).

(2) The renewal conditions are—

(a) that the Secretary of State considers that the warrant continues to be necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within section 178(2),

(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,

(c) that the Secretary of State considers that—

(i) each of the specified operational purposes (see section 183) is a purpose for which the examination of material obtained under the warrant continues to be, or may be, necessary, and

(ii) the examination of such material for each such purpose continues to be necessary on any of the grounds on which the Secretary of State considers that the warrant continues to be necessary, and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) "The renewal period" means—

(a) in the case of an urgent warrant which has not been renewed, the relevant period;

(b) in any other case, the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect.

(4) The decision to renew a bulk equipment interference warrant must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(5) Section 179 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a bulk equipment interference warrant as it applies in relation to a decision to issue a bulk equipment interference warrant.

This is subject to subsection (6).

(6) In the case of a bulk equipment interference warrant which has been modified so that it no longer authorises or requires the securing of interference with any equipment or the obtaining of any communications, equipment data or other information—

(a) the renewal condition in subsection (2)(a) is to be disregarded,

(b) the reference in subsection (2)(c)(ii) to the grounds on which the Secretary of State considers the warrant to be necessary is to be read as a reference to any grounds falling within section 178(1)(b) or (2), and

(c) section 179 has effect as if—

(i) paragraph (a) of subsection (1) were omitted, and

(ii) the reference in subsection (1)(c)(ii) to the grounds on which the Secretary of State considers the warrant to be necessary were a reference to any grounds falling within section 178(1)(b) or (2).

(7) In this section—

"the relevant period" has the same meaning as in section 184;

"urgent warrant" is to be read in accordance with subsection (3) of that section.

186 Modification of warrants

(1) The provisions of a bulk equipment interference warrant may be modified at any time by an instrument issued by the person making the modification.

(2) The modifications which may be made under this section are—

(a) adding, varying or removing any operational purpose specified in the warrant as a purpose for which any material obtained under the warrant may be selected for examination, and

(b) adding, varying or removing any description of conduct authorised by the warrant.

(3) In this section—

(a) a modification adding or varying any operational purpose, or any description of conduct, as mentioned in subsection (2) is referred to as a "major modification", and

(b) any other modification within that subsection is referred to as a "minor modification".

(4) A major modification adding or varying any operational purpose—

(a) must be made by the Secretary of State, and

(b) may be made only if the Secretary of State considers that it is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary (see section 178(1)(b)).

(5) A major modification adding or varying any description of conduct—

(a) must be made by the Secretary of State, and

(b) may be made only if the Secretary of State considers—

(i) that the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary (see section 178(1)(b)), and

(ii) that the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct.

(6) Except where the Secretary of State considers that there is an urgent need to make the modification, a major modification has effect only if the decision to make the modification is approved by a Judicial Commissioner.

(7) A minor modification may be made by—

(a) the Secretary of State, or

(b) a senior official acting on behalf of the Secretary of State.

(8) Where a minor modification is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

(9) If at any time a person mentioned in subsection (7) considers that any operational purpose specified in a warrant is no longer a purpose for which the examination of material obtained under the warrant is or may be necessary, the person must modify the warrant by removing that operational purpose.

(10) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

This is subject to subsection (11).

(11) If it is not reasonably practicable for an instrument making a major modification to be signed by the Secretary of State, the instrument may be signed by a senior official designated by the Secretary of State for that purpose.

(12) In such a case, the instrument making the modification must contain a statement that—

(a) it is not reasonably practicable for the instrument to be signed by the Secretary of State, and

(b) the Secretary of State has personally and expressly authorised the making of the modification.

(13) Despite section 176(1)(b) and (4)(a), the modification of a bulk equipment interference warrant so that it no longer authorises or requires the securing of interference with any equipment or the obtaining of any communications, equipment data or other information does not prevent the warrant from being a bulk equipment interference warrant.

(14) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised by it.

187 Approval of major modifications by Judicial Commissioners

(1) In deciding whether to approve a decision to make a major modification of a bulk equipment interference warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary, and

(b) in the case of a major modification adding or varying any description of conduct authorised by the warrant, whether the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to make a major modification under section 186, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to make a major modification under section 186, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to make the modification.

188 Approval of major modifications made in urgent cases

(1) This section applies where—

(a) the Secretary of State makes a major modification of a bulk equipment interference warrant without the approval of a Judicial Commissioner, and

(b) the Secretary of State considered that there was an urgent need to make the modification.

(2) The Secretary of State must inform a Judicial Commissioner that the modification has been made.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to make the modification, and

(b) notify the Secretary of State of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the modification was made.

(4) If the Judicial Commissioner refuses to approve the decision to make the modification—

(a) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and

(b) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant by virtue of that modification stops as soon as possible,

and section 187(4) does not apply in relation to the refusal to approve the decision.

(5) The Judicial Commissioner may authorise further interference with equipment for the purpose of enabling the person to whom the warrant is addressed to secure that anything in the process of being done under the warrant by virtue of the modification stops as soon as possible.

(6) Nothing in this section affects the lawfulness of—

(a) anything done under the warrant by virtue of the modification before the modification ceases to have effect;

(b) if anything is in the process of being done under the warrant by virtue of the modification when the modification ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done which it is not reasonably practicable to stop.

189 Cancellation of warrants

(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a bulk equipment interference warrant at any time.

(2) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, considers that any of the cancellation conditions are met in relation to a bulk equipment interference warrant, the person must cancel the warrant.

(3) The cancellation conditions are—

(a) that the warrant is no longer necessary in the interests of national security;

(b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct;

(c) that the examination of material obtained under the warrant is no longer necessary for any of the specified operational purposes (see section 183).

(4) But the condition in subsection (3)(a) does not apply where the warrant has been modified so that it no longer authorises or requires the securing of interference with any equipment or the obtaining of any communications, equipment data or other information.

(5) Where a warrant is cancelled under this section, the person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(6) A warrant that has been cancelled under this section may not be renewed.

Implementation of warrants

190 Implementation of warrants

(1) In giving effect to a bulk equipment interference warrant, the person to whom it is addressed ("the implementing authority") may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under subsection (2) or otherwise) to provide the authority with assistance in giving effect to the warrant.

(2) For the purpose of requiring any person to provide assistance in relation to a bulk equipment interference warrant, the implementing authority may—

(a) serve a copy of the warrant on any person who the implementing authority considers may be able to provide such assistance, or

(b) make arrangements for the service of a copy of the warrant on any such person.

(3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(4) For the purposes of this Act, the provision of assistance in giving effect to a bulk equipment interference warrant includes any disclosure to the implementing authority, or to persons acting on behalf of the implementing authority, of material obtained under the warrant.

(5) Sections 127 (service of warrants) and 128 (duty of telecommunications operators to assist with implementation) apply in relation to a bulk equipment interference warrant as they apply in relation to a targeted equipment interference warrant issued under section 102 by the Secretary of State.

(6) References in this section (and in sections 127 and 128 as they apply in relation to bulk equipment interference warrants) to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in the warrant.

Restrictions on use or disclosure of material obtained under warrants etc.

191 Safeguards relating to retention and disclosure of material

(1) The Secretary of State must ensure, in relation to every bulk equipment interference warrant, that arrangements are in force for securing—

(a) that the requirements of subsections (2) and (5) are met in relation to the material obtained under the warrant, and

(b) that the requirements of section 193 are met in relation to that material.

This is subject to subsection (8).

(2) The requirements of this subsection are met in relation to the material obtained under the warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))—

(a) the number of persons to whom any of the material is disclosed or otherwise made available;

(b) the extent to which any of the material is disclosed or otherwise made available;

(c) the extent to which any of the material is copied;

(d) the number of copies that are made.

(3) For the purposes of subsection (2) something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 178(2),

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is or was addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or of the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary for the purpose of legal proceedings, or

(e) it is necessary for the performance of the functions of any person under any enactment.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the material obtained under the warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any relevant grounds for retaining a copy of any material if, and only if—

(a) its retention is not necessary, or not likely to become necessary, in the interests of national security or on any other grounds falling within section 178(2), and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (3) above.

(7) Subsection (8) applies if—

(a) any material obtained under the warrant has been handed over to any overseas authorities, or

(b) a copy of any such material has been given to any overseas authorities.

(8) To the extent that the requirements of subsections (2) and (5) and section 193 relate to any of the material mentioned in subsection (7)(a), or to the copy mentioned in subsection (7)(b), the arrangements made for the purpose of this section are not required to secure that those requirements are met (see instead section 192).

(9) In this section—

"copy", in relation to any material obtained under a warrant, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the material which identifies the material as having been obtained under the warrant, and

(b) any record which is a record of the identities of persons who owned, used or were in possession of the equipment which was interfered with to obtain that material,

and "copied" is to be read accordingly;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

192 Safeguards relating to disclosure of material overseas

(1) The Secretary of State must ensure, in relation to every bulk equipment interference warrant, that arrangements are in force for securing that—

(a) any material obtained under the warrant is handed over to overseas authorities only if the requirements of subsection (2) are met, and

(b) copies of any such material are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of a warrant if it appears to the Secretary of State that requirements corresponding to the requirements of

section 191(2) and (5) and section 193 will apply, to such extent (if any) as the Secretary of State considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question.

(3) In this section—

"copy" has the same meaning as in section 191;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

193 Safeguards relating to examination of material etc.

(1) For the purposes of section 191, the requirements of this section are met in relation to the material obtained under a warrant if—

(a) the selection of any of the material obtained under the warrant for examination is carried out only for the specified purposes (see subsection (2)),

(b) the selection of any of the material for examination is necessary and proportionate in all the circumstances, and

(c) where any such material is protected material, the selection of the material for examination meets any of the selection conditions (see subsection (3)).

(2) The selection of material obtained under the warrant for examination is carried out only for the specified purposes if the material is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 183.

In this subsection "specified in the warrant" means specified in the warrant at the time of the selection of the material for examination.

(3) The selection conditions referred to in subsection (1)(c) are—

(a) that the selection of the protected material for examination does not breach the prohibition in subsection (4);

(b) that the person to whom the warrant is addressed reasonably considers that the selection of the protected material for examination would not breach that prohibition;

(c) that the selection of the protected material for examination in breach of that prohibition is authorised by subsection (5);

(d) that the selection of the protected material for examination in breach of that prohibition is authorised by a targeted examination warrant issued under Part 5.

(4) The prohibition referred to in subsection (3)(a) is that the protected material may not at any time be selected for examination if—

(a) any criteria used for the selection of the material for examination are referable to an individual known to be in the British Islands at that time, and

(b) the purpose of using those criteria is to identify protected material consisting of communications sent by, or intended for, that individual or private information relating to that individual.

It does not matter for the purposes of this subsection whether the identity of the individual is known.

(5) The selection of protected material ("the relevant material") for examination is authorised by this subsection if—

(a) criteria referable to an individual have been, or are being, used for the selection of material for examination in circumstances falling within subsection (3)(a) or (b),

(b) at any time it appears to the person to whom the warrant is addressed that there has been a relevant change of circumstances in relation to the individual (see subsection (6)) which would mean that the selection of the relevant material for examination would breach the prohibition in subsection (4),

(c) since that time, a written authorisation to examine the relevant material using those criteria has been given by a senior officer, and

(d) the selection of the relevant material for examination is made before the end of the permitted period (see subsection (7)).

(6) For the purposes of subsection (5)(b) there is a relevant change of circumstances in relation to an individual if—

(a) the individual has entered the British Islands, or

(b) a belief by the person to whom the warrant is addressed that the individual was outside the British Islands was in fact mistaken.

(7) In subsection (5)—

"senior officer", in relation to a warrant addressed to the head of an intelligence service, means a member of the intelligence service who—

(a) is a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service, or

(b) holds a position in the intelligence service of equivalent seniority to such a member;

"the permitted period" means the period ending with the fifth working day after the time mentioned in subsection (5)(b).

(8) In a case where the selection of protected material for examination is authorised by subsection (5), the person to whom the warrant is addressed must notify the Secretary of State that the selection is being carried out.

(9) In this Part, "protected material" means any material obtained under the warrant other than material which is—

(a) equipment data;

(b) information (other than a communication or equipment data) which is not private information.

194 Additional safeguards for items subject to legal privilege

(1) Subsection (2) applies if, in a case where protected material obtained under a bulk equipment interference warrant is to be selected for examination—

(a) the selection of the material for examination meets any of the selection conditions in section 193(3)(a) to (c), and

(b) either—

(i) the purpose, or one of the purposes, of using the criteria to be used for the selection of the material for examination ("the relevant criteria") is to identify any items subject to legal privilege, or

(ii) the use of the relevant criteria is likely to identify such items.

(2) The material may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(3) In deciding whether to give an approval under subsection (2) in a case where subsection (1)(b)(i) applies, a senior official must have regard to the public interest in the confidentiality of items subject to legal privilege.

(4) A senior official may give an approval under subsection (2) only if—

(a) the official considers that the arrangements made for the purposes of section 191 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege, and

(b) where subsection (1)(b)(i) applies, the official considers that there are exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria.

(5) For the purposes of subsection (4)(b), there cannot be exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria unless—

(a) the public interest in obtaining the information that would be obtained by the selection of the material for examination outweighs the public interest in the confidentiality of items subject to legal privilege,

(b) there are no other means by which the information may reasonably be obtained, and

(c) obtaining the information is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(6) Subsection (7) applies if, in a case where protected material obtained under a bulk equipment interference warrant is to be selected for examination—

(a) the selection of the material for examination meets any of the selection conditions in section 193(3)(a) to (c),

(b) the purpose, or one of the purposes, of using the criteria to be used for the selection of the material for examination ("the relevant criteria") is to identify communications or other items of information that, if they were not communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose, would be items subject to legal privilege, and

(c) the person to whom the warrant is addressed considers that the communications or other items of information ("the targeted communications or other items of information") are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

(7) The material may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(8) A senior official may give an approval under subsection (7) only if the official considers that the targeted communications or other items of information are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

(9) Where an item subject to legal privilege which has been obtained under a bulk equipment interference warrant is retained following its examination, for purposes other than the destruction of the item, the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

(For provision about the grounds for retaining material obtained under a bulk equipment interference warrant, see section 191.)

(10) Unless the Investigatory Powers Commissioner considers that subsection (12) applies to the item, the Commissioner must—

(a) direct that the item is destroyed, or

(b) impose one or more conditions as to the use or retention of that item.

(11) If the Investigatory Powers Commissioner considers that subsection (12) applies to the item, the Commissioner may nevertheless impose such conditions under subsection (10)(b) as the Commissioner considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege.

(12) This subsection applies to an item subject to legal privilege if—

(a) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and

(b) retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(13) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsection (10), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(14) Each of the following is an "affected party" for the purposes of subsection (13)—

(a) the Secretary of State;

(b) the person to whom the warrant is or was addressed.

195 Additional safeguard for confidential journalistic material

Where—

(a) material obtained under a bulk equipment interference warrant is retained, following its examination, for purposes other than the destruction of the material, and

(b) it is material containing confidential journalistic material,

the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

196 Offence of breaching safeguards relating to examination of material

(1) A person commits an offence if—

(a) the person selects for examination any material obtained under a bulk equipment interference warrant,

(b) the person knows or believes that the selection of that material does not comply with a requirement imposed by section 193 or 194, and

(c) the person deliberately selects that material in breach of that requirement.

(2) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(3) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

197 Application of other restrictions in relation to warrants

Sections 132 to 134 (duty not to make unauthorised disclosures) apply in relation to bulk equipment interference warrants as they apply in relation to targeted equipment interference warrants, but as if the reference in section 133(2)(c) to a requirement for disclosure imposed by virtue of section 126(4) were a reference to such a requirement imposed by virtue of section 190(4).

Interpretation

198 Chapter 3: interpretation

(1) In this Chapter—

"communication" includes—

(a) anything comprising speech, music, sounds, visual images or data of any description, and

(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;

"equipment" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment;

"equipment data" has the meaning given by section 177;

"private information" includes information relating to a person's private or family life;

"protected material", in relation to a bulk equipment interference warrant, has the meaning given by section 193(9);

"senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

"the specified operational purposes" has the meaning given by section 183(12).

(2) See also—

section 261 (telecommunications definitions);

section 263 (general definitions);

section 264 (general definitions: "journalistic material" etc.);

section 265 (index of defined expressions).

PART 7

BULK PERSONAL DATASET WARRANTS

Bulk personal datasets: interpretation

199 Bulk personal datasets: interpretation

(1) For the purposes of this Part, an intelligence service retains a bulk personal dataset if—

(a) the intelligence service obtains a set of information that includes personal data relating to a number of individuals,

(b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions,

(c) after any initial examination of the contents, the intelligence service retains the set for the purpose of the exercise of its functions, and

(d) the set is held, or is to be held, electronically for analysis in the exercise of those functions.

(2) In this Part, "personal data" has the same meaning as in the Data Protection Act 1998 except that it also includes data relating to a deceased individual where the data would be personal data within the meaning of that Act if it related to a living individual.

Requirement for warrant

200 Requirement for authorisation by warrant: general

(1) An intelligence service may not exercise a power to retain a bulk personal dataset unless the retention of the dataset is authorised by a warrant under this Part.

(2) An intelligence service may not exercise a power to examine a bulk personal dataset retained by it unless the examination is authorised by a warrant under this Part.

(3) For the purposes of this Part, there are two kinds of warrant—

(a) a warrant, referred to in this Part as "a class BPD warrant", authorising an intelligence service to retain, or to retain and examine, any bulk personal dataset of a class described in the warrant;

(b) a warrant, referred to in this Part as "a specific BPD warrant", authorising an intelligence service to retain, or to retain and examine, any bulk personal dataset described in the warrant.

(4) Section 201 sets out exceptions to the restrictions imposed by subsections (1) and (2) of this section.

201 Exceptions to section 200(1) and (2)

(1) Section 200(1) or (2) does not apply to the exercise of a power of an intelligence service to retain or (as the case may be) examine a bulk personal dataset if the intelligence service obtained the bulk personal dataset under a warrant or other authorisation issued or given under this Act.

(2) Section 200(1) or (2) does not apply at any time when a bulk personal dataset is being retained or (as the case may be) examined for the purpose of enabling any of the information contained in it to be destroyed.

(3) Sections 210(8), 219(8) and 220(5) provide for other exceptions to section 200(1) or (2) (in connection with cases where a Judicial Commissioner refuses to approve a specific BPD warrant, the non-renewal or cancellation of BPD warrants and initial examinations).

202 Restriction on use of class BPD warrants

(1) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service considers that the bulk personal dataset consists of, or includes, protected data.

For the meaning of "protected data", see section 203.

(2) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service considers—

(a) that the bulk personal dataset consists of, or includes, health records, or

(b) that a substantial proportion of the bulk personal dataset consists of sensitive personal data.

(3) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service considers that the nature of the bulk personal dataset, or the circumstances in which it was created, is or are such that its retention, or retention and examination, by the intelligence service raises novel or contentious issues which ought to be considered by the Secretary of State and a Judicial Commissioner on an application by the head of the intelligence service for a specific BPD warrant.

(4) In subsection (2)—

"health records" has the same meaning as in section 206;

"sensitive personal data" means personal data consisting of information about an individual (whether living or deceased) which is of a kind mentioned in section 2(a) to (f) of the Data Protection Act 1998.

203 Meaning of "protected data"

(1) In this Part, "protected data" means any data contained in a bulk personal dataset other than data which is one or more of the following—

(a) systems data;

(b) data which falls within subsection (2);

(c) data which is not private information.

(2) The data falling within this subsection is identifying data which—

(a) is contained in the bulk personal dataset,

(b) is capable of being logically separated from the bulk personal dataset, and

(c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of any of the data which would remain in the bulk personal dataset or of the bulk personal dataset itself, disregarding any meaning arising from the existence of that data or (as the case may be) the existence of the bulk personal dataset or from any data relating to that fact.

(3) For the meaning of "systems data" see section 263(4).

(4) In this section, "private information" includes information relating to a person's private or family life.

Issue of warrants

204 Class BPD warrants

(1) The head of an intelligence service, or a person acting on his or her behalf, may apply to the Secretary of State for a class BPD warrant.

(2) The application must include—

(a) a description of the class of bulk personal datasets to which the application relates, and

(b) in a case where the intelligence service is seeking authorisation for the examination of bulk personal datasets of that class, the operational purposes which it is proposing should be specified in the warrant (see section 212).

(3) The Secretary of State may issue the warrant if—

(a) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security,

(ii) for the purposes of preventing or detecting serious crime, or

(iii) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by the conduct,

(c) where the warrant authorises the examination of bulk personal datasets of the class described in the warrant, the Secretary of State considers that—

(i) each of the specified operational purposes (see section 212) is a purpose for which the examination of bulk personal datasets of that class is or may be necessary, and

(ii) the examination of bulk personal datasets of that class for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary,

(d) the Secretary of State considers that the arrangements made by the intelligence service for storing bulk personal datasets of the class to which the application relates and for protecting them from unauthorised disclosure are satisfactory, and

(e) the decision to issue the warrant has been approved by a Judicial Commissioner.

(4) The fact that a class BPD warrant would authorise the retention, or the retention and examination, of bulk personal datasets relating to activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on grounds falling within subsection (3)(a).

(5) An application for a class BPD warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

205 Specific BPD warrants

(1) The head of an intelligence service, or a person acting on his or her behalf, may apply to the Secretary of State for a specific BPD warrant in the following cases.

(2) Case 1 is where—

(a) the intelligence service is seeking authorisation to retain, or to retain and examine, a bulk personal dataset, and

(b) the bulk personal dataset does not fall within a class described in a class BPD warrant.

(3) Case 2 is where—

(a) the intelligence service is seeking authorisation to retain, or to retain and examine, a bulk personal dataset, and

(b) the bulk personal dataset falls within a class described in a class BPD warrant but either—

(i) the intelligence service is prevented by section 202(1), (2) or (3) from retaining, or retaining and examining, the bulk personal dataset in reliance on the class BPD warrant, or

(ii) the intelligence service at any time considers that it would be appropriate to seek a specific BPD warrant.

(4) The application must include—

(a) a description of the bulk personal dataset to which the application relates, and

(b) in a case where the intelligence service is seeking authorisation for the examination of the bulk personal dataset, the operational purposes which it is proposing should be specified in the warrant (see section 212).

(5) Where subsection (3)(b)(i) applies, the application must include an explanation of why the intelligence service is prevented by section 202(1), (2) or (3) from retaining, or retaining and examining, the bulk personal dataset in reliance on a class BPD warrant.

(6) The Secretary of State may issue the warrant if—

(a) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security,

(ii) for the purposes of preventing or detecting serious crime, or

(iii) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by the conduct,

(c) where the warrant authorises the examination of a bulk personal dataset, the Secretary of State considers that—

(i) each of the specified operational purposes (see section 212) is a purpose for which the examination of the bulk personal dataset is or may be necessary, and

(ii) the examination of the bulk personal dataset for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary,

(d) the Secretary of State considers that the arrangements made by the intelligence service for storing the bulk personal dataset and for protecting it from unauthorised disclosure are satisfactory, and

(e) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue it has been approved by a Judicial Commissioner.

(7) The fact that a specific BPD warrant would authorise the retention, or the retention and examination, of bulk personal datasets relating to activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on grounds falling within subsection (6)(a).

(8) A specific BPD warrant relating to a bulk personal dataset ("dataset A") may also authorise the retention or examination of other bulk personal datasets ("replacement datasets") that do not exist at the time of the issue of the warrant but may reasonably be regarded as replacements for dataset A.

(9) An application for a specific BPD warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

206 Additional safeguards for health records

(1) Subsections (2) and (3) apply if—

(a) an application is made by or on behalf of the head of an intelligence service for the issue of a specific BPD warrant, and

(b) the purpose, or one of the purposes, of the warrant is to authorise the retention, or the retention and examination, of health records.

(2) The application must contain a statement that the purpose, or one of the purposes, of the warrant is to authorise the retention, or the retention and examination, of health records.

(3) The Secretary of State may issue the warrant only if the Secretary of State considers that there are exceptional and compelling circumstances that make it necessary to authorise the retention, or the retention and examination, of health records.

(4) Subsection (5) applies if—

(a) an application is made by or on behalf of the head of an intelligence service for a specific BPD warrant,

(b) the head of the intelligence service considers that the bulk personal dataset includes, or is likely to include, health records, and

(c) subsections (2) and (3) do not apply.

(5) The application must contain either—

(a) a statement that the head of the intelligence service considers that the bulk personal dataset includes health records, or

(b) a statement that the head of the intelligence service considers that it is likely that the bulk personal dataset includes health records and an assessment of how likely this is.

(6) In this section, "health record" means a record, or a copy of a record, which—

(a) consists of information relating to the physical or mental health or condition of an individual,

(b) was made by or on behalf of a health professional in connection with the care of that individual, and

(c) was obtained by the intelligence service from a health professional or a health service body or from a person acting on behalf of a health professional or a health service body in relation to the record or the copy.

(7) In subsection (6)—

"health professional" has the same meaning as in the Data Protection Act 1998 (see section 69 of that Act);

"health service body" has the meaning given by section 69(3) of that Act.

207 Protected data: power to impose conditions

Where the Secretary of State decides to issue a specific BPD warrant, the Secretary of State may impose conditions which must be satisfied before protected data retained in reliance on the warrant may be selected for examination on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection.

208 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a decision to issue a class BPD warrant or a specific BPD warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the warrant is necessary on grounds falling within section 204(3)(a) or (as the case may be) section 205(6)(a),

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, and

(c) where the warrant authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, whether—

(i) each of the specified operational purposes (see section 212) is a purpose for which the examination of bulk personal datasets of that class or (as the case may be) the bulk personal dataset is or may be necessary, and

(ii) the examination of bulk personal datasets of that class or (as the case may be) the bulk personal dataset is necessary as mentioned in section 204(3)(c)(ii) or (as the case may be) section 205(6)(c)(ii).

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to issue a class BPD warrant or a specific BPD warrant, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a class BPD warrant or a specific BPD warrant, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

209 Approval of specific BPD warrants issued in urgent cases

(1) This section applies where—

(a) a specific BPD warrant is issued without the approval of a Judicial Commissioner, and

(b) the Secretary of State considered that there was an urgent need to issue it.

(2) The Secretary of State must inform a Judicial Commissioner that it has been issued.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to issue the warrant, and

(b) notify the Secretary of State of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the warrant was issued.

(4) If a Judicial Commissioner refuses to approve the decision to issue a specific BPD warrant, the warrant—

(a) ceases to have effect (unless already cancelled), and

(b) may not be renewed,

and section 208(4) does not apply in relation to the refusal to approve the decision.

(5) Section 210 contains further provision about what happens if a Judicial Commissioner refuses to approve a decision to issue a warrant.

210 Failure to approve specific BPD warrant issued in urgent case

(1) This section applies where under section 209(3) a Judicial Commissioner refuses to approve the decision to issue a warrant.

(2) The head of the intelligence service to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done in reliance on the warrant stops as soon as possible.

(3) The Judicial Commissioner may—

(a) direct that the whole or part of a bulk personal dataset retained in reliance on the warrant is destroyed;

(b) impose conditions as to the use or retention of the whole or part of any such bulk personal dataset.

(4) The Judicial Commissioner—

(a) may require an affected party to make representations about how the Judicial Commissioner should exercise any function under subsection (3), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(5) Each of the following is an "affected party" for the purposes of subsection (4)—

(a) the Secretary of State;

(b) the head of the intelligence service to whom the warrant was addressed.

(6) The Secretary of State may ask the Investigatory Powers Commissioner to review a decision made by any other Judicial Commissioner under subsection (3).

(7) On a review under subsection (6), the Investigatory Powers Commissioner may—

(a) confirm the Judicial Commissioner's decision, or

(b) make a fresh determination.

(8) An intelligence service is not to be regarded as in breach of section 200(1) or (2) where it retains or (as the case may be) examines a bulk personal dataset in accordance with conditions imposed under subsection (3)(b).

(9) Nothing in this section or section 209 affects the lawfulness of—

(a) anything done in reliance on the warrant before it ceases to have effect;

(b) if anything is in the process of being done in reliance on the warrant when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done that it is not reasonably practicable to stop.

211 Decisions to issue warrants to be taken personally by Secretary of State

(1) The decision to issue a class BPD warrant or a specific BPD warrant must be taken personally by the Secretary of State.

(2) Before a class BPD warrant is issued, it must be signed by the Secretary of State.

(3) Before a specific BPD warrant is issued, it must be signed by the Secretary of State (subject to subsection (4)).

(4) If it is not reasonably practicable for a specific BPD warrant to be signed by the Secretary of State, it may be signed by a senior official designated by the Secretary of State for that purpose.

(5) In such a case, the warrant must contain a statement that—

(a) it is not reasonably practicable for the warrant to be signed by the Secretary of State, and

(b) the Secretary of State has personally and expressly authorised the issue of the warrant.

212 Requirements that must be met by warrants

(1) A class BPD warrant or a specific BPD warrant must contain a provision stating whether it is a class BPD warrant or (as the case may be) a specific BPD warrant.

(2) A class BPD warrant or a specific BPD warrant must be addressed to the head of the intelligence service by whom, or on whose behalf, the application for the warrant was made.

(3) A class BPD warrant must—

(a) include a description of the class of bulk personal datasets to which the warrant relates, and

(b) where the warrant authorises examination of bulk personal datasets of that class, specify the operational purposes for which data contained in bulk personal datasets of that class may be selected for examination.

(4) A specific BPD warrant must—

(a) describe the bulk personal dataset to which the warrant relates,

(b) where the warrant authorises the retention or examination of replacement datasets, include a description that will enable those datasets to be identified,

(c) where the warrant authorises the examination of the bulk personal dataset or replacement datasets, specify the operational purposes for which data contained in the bulk personal dataset and any replacement datasets may be selected for examination, and

(d) where the Secretary of State has imposed conditions under section 207, specify those conditions.

(5) The operational purposes specified in a class BPD warrant or a specific BPD warrant must be ones specified, in a list maintained by the heads of the intelligence services ("the list of operational purposes"), as purposes which they consider are operational purposes for which data contained in bulk personal datasets retained in reliance on class BPD warrants or specific BPD warrants may be selected for examination.

(6) A class BPD warrant or a specific BPD warrant may, in particular, specify all of the operational purposes which, at the time the warrant is issued, are specified in the list of operational purposes.

(7) An operational purpose may be specified in the list of operational purposes only with the approval of the Secretary of State.

(8) The Secretary of State may give such approval only if satisfied that the operational purpose is specified in a greater level of detail than the descriptions contained in section 204(3)(a) or (as the case may be) section 205(6)(a).

(9) At the end of each relevant three-month period, the Secretary of State must give a copy of the list of operational purposes to the Intelligence and Security Committee of Parliament.

(10) In subsection (9), "relevant three-month period" means—

(a) the period of three months beginning with the day on which this section comes into force, and

(b) each successive period of three months.

(11) The Prime Minister must review the list of operational purposes at least once a year.

(12) In this Part, "the specified operational purposes", in relation to a class BPD warrant or a specific BPD warrant, means the operational purposes specified in the warrant in accordance with this section.

Duration, modification and cancellation

213 Duration of warrants

(1) A class BPD warrant or a specific BPD warrant ceases to have effect at the end of the relevant period (see subsection (2)) unless—

(a) it is renewed before the end of that period (see section 214), or

(b) it is cancelled or (in the case of a specific BPD warrant) otherwise ceases to have effect before the end of that period (see sections 209 and 218).

(2) In this section, "the relevant period"—

(a) in the case of an urgent specific BPD warrant (see subsection (3)), means the period ending with the fifth working day after the day on which the warrant was issued;

(b) in any other case, means the period of 6 months beginning with—

(i) the day on which the warrant was issued, or

(ii) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) For the purposes of subsection (2)(a), a specific BPD warrant is an "urgent specific BPD warrant" if—

(a) the warrant was issued without the approval of a Judicial Commissioner, and

(b) the Secretary of State considered that there was an urgent need to issue it.

(4) For provision about the renewal of warrants, see section 214.

214 Renewal of warrants

(1) If the renewal conditions are met, a class BPD warrant or a specific BPD warrant may be renewed, at any time during the renewal period, by an instrument issued by the Secretary of State.

(2) The renewal conditions are—

(a) that the Secretary of State considers that the warrant continues to be necessary on grounds falling within section 204(3)(a) or (as the case may be) section 205(6)(a),

(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by the conduct,

(c) where the warrant authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, that the Secretary of State considers that—

(i) each of the specified operational purposes (see section 212) is a purpose for which the examination of bulk personal datasets of that class or (as the case may be) the bulk personal dataset continues to be, or may be, necessary, and

(ii) the examination of bulk personal datasets of that class or (as the case may be) the bulk personal dataset continues to be necessary on any of the grounds on which the Secretary of State considers that the warrant continues to be necessary, and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) "The renewal period" means—

(a) in the case of an urgent specific BPD warrant which has not been renewed, the relevant period;

(b) in any other case, the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect.

(4) The decision to renew a class BPD warrant or a specific BPD warrant must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(5) Section 207 (protected data: power to impose conditions) applies in relation to the renewal of a specific BPD warrant as it applies in relation to the issue of such a warrant (whether or not any conditions have previously been imposed in relation to the warrant under that section).

(6) Section 208 (approval of warrants by Judicial Commissioner) applies in relation to a decision to renew a warrant as it applies in relation to a decision to issue a warrant.

(7) In this section—

"the relevant period" has the same meaning as in section 213;

"urgent specific BPD warrant" is to be read in accordance with subsection (3) of that section.

215 Modification of warrants

(1) The provisions of a class BPD warrant or a specific BPD warrant may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications which may be made under this section are—

(a) in the case of a class BPD warrant, adding, varying or removing any operational purpose specified in the warrant as a purpose for which bulk personal datasets of a class described in the warrant may be examined;

(b) in the case of a specific BPD warrant, adding, varying or removing any operational purpose specified in the warrant as a purpose for which the bulk personal dataset described in the warrant may be examined.

(3) In this section—

(a) a modification adding or varying any operational purpose is referred to as a "major modification", and

(b) a modification removing any operational purpose is referred to as a "minor modification".

(4) A major modification—

(a) must be made by the Secretary of State, and

(b) may be made only if the Secretary of State considers that it is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary (see section 204(3)(a) or (as the case may be) section 205(6)(a)).

(5) Except where the Secretary of State considers that there is an urgent need to make the modification, a major modification has effect only if the decision to make the modification is approved by a Judicial Commissioner.

(6) A minor modification may be made by—

(a) the Secretary of State, or

(b) a senior official acting on behalf of the Secretary of State.

(7) Where a minor modification is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

(8) If at any time a person mentioned in subsection (6) considers that any operational purpose specified in a warrant is no longer a purpose for which the examination of any bulk personal datasets to which the warrant relates is or may be necessary, the person must modify the warrant by removing that operational purpose.

(9) The decision to modify the provisions of a class BPD warrant or a specific BPD warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

This is subject to subsection (10).

(10) If it is not reasonably practicable for an instrument making a major modification to be signed by the Secretary of State, the instrument may be signed by a senior official designated by the Secretary of State for that purpose.

(11) In such a case, the instrument making the modification must contain a statement that—

(a) it is not reasonably practicable for the instrument to be signed by the Secretary of State, and

(b) the Secretary of State has personally and expressly authorised the making of the modification.

216 Approval of major modifications by Judicial Commissioners

(1) In deciding whether to approve a decision to make a major modification of a class BPD warrant or a specific BPD warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to make a major modification under section 215, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to make a major modification under section 215, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to make the modification.

217 Approval of major modifications made in urgent cases

(1) This section applies where—

(a) the Secretary of State makes a major modification of a class BPD warrant or a specific BPD warrant without the approval of a Judicial Commissioner, and

(b) the Secretary of State considered that there was an urgent need to make the modification.

(2) The Secretary of State must inform a Judicial Commissioner that the modification has been made.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to make the modification, and

(b) notify the Secretary of State of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the modification was made.

(4) If the Judicial Commissioner refuses to approve the decision to make the modification—

(a) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and

(b) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done in reliance on the warrant by virtue of that modification stops as soon as possible,

and section 216(4) does not apply in relation to the refusal to approve the decision.

(5) Nothing in this section affects the lawfulness of—

(a) anything done in reliance on the warrant by virtue of the modification before the modification ceases to have effect;

(b) if anything is in the process of being done in reliance on the warrant by virtue of the modification when the modification ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done which it is not reasonably practicable to stop.

218 Cancellation of warrants

(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a class BPD warrant or a specific BPD warrant at any time.

(2) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, considers that any of the cancellation conditions are met in relation to a class BPD warrant or a specific BPD warrant, the person must cancel the warrant.

(3) The cancellation conditions are—

(a) that the warrant is no longer necessary on any grounds falling within section 204(3)(a) or (as the case may be) section 205(6)(a);

(b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct;

(c) where the warrant authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, that the examination of bulk personal datasets of that class or (as the case may be) of the bulk personal dataset is no longer necessary for any of the specified operational purposes (see section 212).

219 Non-renewal or cancellation of BPD warrants

(1) This section applies where a class BPD warrant or a specific BPD warrant ceases to have effect because it expires without having been renewed or because it is cancelled.

(2) The head of the intelligence service to whom the warrant was addressed may, before the end of the period of 5 working days beginning with the day on which the warrant ceases to have effect—

(a) apply for—

(i) a specific BPD warrant authorising the retention, or the retention and examination, of the whole or any part of the material retained by the intelligence service in reliance on the warrant which has ceased to have effect;

(ii) a class BPD warrant authorising the retention or (as the case may be) the retention and examination of bulk personal datasets of a class that is described in a way that would authorise the retention or (as the case may be) the retention and examination of the whole or any part of such material, or

(b) where the head of the intelligence service wishes to give further consideration to whether to apply for a warrant of a kind mentioned in paragraph (a)(i) or (ii), apply to the Secretary of State for authorisation to retain, or to retain and examine, the whole or any part of the material retained by the intelligence service in reliance on the warrant.

(3) On an application under subsection (2)(b), the Secretary of State may—

(a) direct that any of the material to which the application relates be destroyed;

(b) with the approval of a Judicial Commissioner, authorise the retention or (as the case may be) the retention and examination of any of that material, subject to such conditions as the Secretary of State considers appropriate, for a period specified by the Secretary of State which may not exceed 3 months.

(4) In deciding whether to give approval for the purposes of subsection (3)(b), the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(5) Where a Judicial Commissioner refuses to approve a decision by the Secretary of State to authorise the retention or (as the case may be) the retention and examination of any material under subsection (3)(b), the Judicial Commissioner must give the Secretary of State written reasons for the decision.

(6) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve such a decision, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision.

(7) If, during the period specified by the Secretary of State under subsection (3)(b), the head of the intelligence service decides to apply for a warrant of a kind mentioned in subsection (2)(a)(i) or (ii), the head of the intelligence service must make the application as soon as reasonably practicable and before the end of the period specified by the Secretary of State.

(8) Where a class BPD warrant or a specific BPD warrant ceases to have effect because it expires without having been renewed or it is cancelled, an intelligence service is not to be regarded as in breach of section 200(1) or (2) by virtue of its retention or examination of any material to which the warrant related during any of the following periods.

First period

The period of 5 working days beginning with the day on which the warrant ceases to have effect.

Second period

The period beginning with the day on which the head of the intelligence service makes an application under subsection (2)(a) or (b) in relation to the material and ending with the determination of the application.

Third period

The period during which the retention or examination of the material is authorised under subsection (3)(b).

Fourth period

Where authorisation under subsection (3)(b) is given and the head of the intelligence service subsequently makes, in accordance with subsection (7), an application for a specific BPD warrant or a class BPD warrant in relation to the material, the period (if any) beginning with the expiry of the authorisation under subsection (3)(b) and ending with the determination of the application for the warrant.

Further and supplementary provision

220 Initial examinations: time limits

(1) This section applies where—

(a) an intelligence service obtains a set of information otherwise than in the exercise of a power conferred by a warrant or other authorisation issued or given under this Act, and

(b) the head of the intelligence service believes that—

(i) the set includes, or may include, personal data relating to a number of individuals, and

(ii) the nature of the set is, or may be, such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions.

(2) The head of the intelligence service must take the following steps before the end of the permitted period.

Step 1

Carry out an initial examination of the set for the purpose of deciding whether, if the intelligence service were to retain it after that initial examination and hold it electronically for analysis for the purposes of the exercise of its functions, the intelligence service would be retaining a bulk personal dataset (see section 199).

Step 2

If the intelligence service would be retaining a bulk personal dataset as mentioned in step 1, decide whether to retain the set and hold it electronically for analysis for the purposes of the exercise of the functions of the intelligence service.

Step 3

If the head of the intelligence service decides to retain the set and hold it electronically for analysis as mentioned in step 2, apply for a specific BPD warrant as soon as reasonably practicable after making that decision (unless the retention of the dataset is authorised by a class BPD warrant).

(3) The permitted period begins when the head of the intelligence service first forms the beliefs mentioned in subsection (1)(b).

(4) The permitted period ends—

(a) where the set of information was created in the United Kingdom, 3 months after the day on which it begins;

(b) where the set of information was created outside the United Kingdom, 6 months after the day on which it begins.

(5) If the head of the intelligence service applies for a specific BPD warrant in accordance with step 3 (set out in subsection (2))—

(a) the intelligence service is not to be regarded as in breach of section 200(1) by virtue of retaining the bulk personal dataset during the period between the taking of the decision mentioned in step 2 and the determination of the application for the specific BPD warrant, and

(b) the intelligence service is not to be regarded as in breach of section 200(2) by virtue of examining the bulk personal dataset during that period if the examination is necessary for the purposes of the making of the application for the warrant.

221 Safeguards relating to examination of bulk personal datasets

(1) The Secretary of State must ensure, in relation to every class BPD warrant or specific BPD warrant which authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, that arrangements are in force for securing that—

(a) any selection of data contained in the datasets (or dataset) for examination is carried out only for the specified purposes (see subsection (2)), and

(b) the selection of any such data for examination is necessary and proportionate in all the circumstances.

(2) The selection of data contained in bulk personal datasets for examination is carried out only for the specified purposes if the data is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 212.

(3) The Secretary of State must also ensure, in relation to every specific BPD warrant which specifies conditions imposed under section 207, that arrangements are in force for securing that any selection for examination of protected data on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection is in accordance with the conditions specified in the warrant.

(4) In this section "specified in the warrant" means specified in the warrant at the time of the selection of the data for examination.

222 Additional safeguards for items subject to legal privilege: examination

(1) Subsections (2) and (3) apply if, in a case where protected data retained in reliance on a specific BPD warrant is to be selected for examination—

(a) the purpose, or one of the purposes, of using the criteria to be used for the selection of the data for examination ("the relevant criteria") is to identify any items subject to legal privilege, or

(b) the use of the relevant criteria is likely to identify such items.

(2) If the relevant criteria are referable to an individual known to be in the British Islands at the time of the selection, the data may be selected for examination using the relevant criteria only if the Secretary of State has approved the use of those criteria.

(3) In any other case, the data may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(4) The Secretary of State may give approval for the purposes of subsection (2) only with the approval of a Judicial Commissioner.

(5) Approval may be given under subsection (2) or (3) only if—

(a) the Secretary of State or (as the case may be) the senior official considers that the arrangements mentioned in section 205(6)(d) include specific arrangements in respect of items subject to legal privilege, and

(b) where subsection (1)(a) applies, the Secretary of State or (as the case may be) the senior official considers that there are exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria.

(6) In deciding whether to give an approval under subsection (2) or (3) in a case where subsection (1)(a) applies, the Secretary of State or (as the case may be) the senior official must have regard to the public interest in the confidentiality of items subject to legal privilege.

(7) For the purposes of subsection (5)(b), there cannot be exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria unless—

(a) the public interest in obtaining the information that would be obtained by the selection of the data for examination outweighs the public interest in the confidentiality of items subject to legal privilege,

(b) there are no other means by which the information may reasonably be obtained, and

(c) obtaining the information is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(8) In deciding whether to give approval for the purposes of subsection (4), the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(9) Subsections (10) and (11) apply if, in a case where protected data retained in reliance on a specific BPD warrant is to be selected for examination—

(a) the purpose, or one of the purposes, of using the criteria to be used for the selection of the data for examination ("the relevant criteria") is to identify data that, if the data or any underlying material were not created or held with the intention of furthering a criminal purpose, would be an item subject to legal privilege, and

(b) the person to whom the warrant is addressed considers that the data ("the targeted data") or any underlying material is likely to be data or underlying material created or held with the intention of furthering a criminal purpose.

(10) If the relevant criteria are referable to an individual known to be in the British Islands at the time of the selection, the data may be selected for examination using the relevant criteria only if the Secretary of State has approved the use of those criteria.

(11) In any other case, the data may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(12) Approval may be given under subsection (10) or (11) only if the Secretary of State or (as the case may be) the senior official considers that the targeted data or the underlying material is likely to be data or underlying material created or held with the intention of furthering a criminal purpose.

(13) In this section, "underlying material", in relation to data retained in reliance on a specific BPD warrant, means any communications or other items of information from which the data was produced.

223 Additional safeguards for items subject to legal privilege: retention following examination

(1) Where an item subject to legal privilege is retained following its examination in reliance on a specific BPD warrant, for purposes other than the destruction of the item, the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

(2) Unless the Investigatory Powers Commissioner considers that subsection (4) applies to the item, the Commissioner must—

(a) direct that the item is destroyed, or

(b) impose one or more conditions as to the use or retention of that item.

(3) If the Investigatory Powers Commissioner considers that subsection (4) applies to the item, the Commissioner may nevertheless impose such conditions under subsection (2)(b) as the Commissioner considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege.

(4) This subsection applies to an item subject to legal privilege if—

(a) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and

(b) retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(5) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsection (2), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(6) Each of the following is an "affected party" for the purposes of subsection (5)—

(a) the Secretary of State;

(b) the person to whom the warrant is or was addressed.

224 Offence of breaching safeguards relating to examination of material

(1) A person commits an offence if—

(a) the person selects for examination any data contained in a bulk personal dataset retained in reliance on a class BPD warrant or a specific BPD warrant,

(b) the person knows or believes that the selection of that data is in breach of a requirement specified in subsection (2), and

(c) the person deliberately selects that data in breach of that requirement.

(2) The requirements specified in this subsection are that any selection for examination of the data—

(a) is carried out only for the specified purposes (see subsection (3)),

(b) is necessary and proportionate, and

(c) if the data is protected data, satisfies any conditions imposed under section 207.

(3) The selection for examination of the data is carried out only for the specified purposes if the data is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 212.

In this subsection, "specified in the warrant" means specified in the warrant at the time of the selection of the data for examination.

(4) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(5) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

225 Application of Part to bulk personal datasets obtained under this Act

(1) Subject to subsection (2), this section applies where a bulk personal dataset has been obtained by an intelligence service under a warrant or other authorisation issued or given under this Act (and, accordingly, section 200(1) and (2) do not apply by virtue of section 201(1)).

(2) This section does not apply where the bulk personal dataset was obtained by the intelligence service under a bulk acquisition warrant issued under Chapter 2 of Part 6.

(3) Where this section applies, the Secretary of State may, on the application of the head of the intelligence service, give a direction that—

(a) the intelligence service may retain, or retain and examine, the bulk personal dataset by virtue of the direction,

(b) any other power of the intelligence service to retain or examine the bulk personal dataset, and any associated regulatory provision, ceases to apply in relation to the bulk personal dataset (subject to subsection (5)), and

(c) section 201(1) also ceases to apply in relation to the bulk personal dataset.

(4) Accordingly, where a direction is given under subsection (3), the intelligence service may exercise its power by virtue of the direction to retain, or to retain and examine, the bulk personal dataset only if authorised to do so by a class BPD warrant or a specific BPD warrant under this Part.

(5) A direction under subsection (3) may provide for any associated regulatory provision specified in the direction to continue to apply in relation to the bulk personal dataset, with or without modifications specified in the direction.

(6) The power conferred by subsection (5) must be exercised to ensure that—

(a) where section 56 and Schedule 3 applied in relation to the bulk personal dataset immediately before the giving of the direction, they continue to apply in relation to it (without modification);

(b) where sections 57 to 59 applied in relation to the bulk personal dataset immediately before the giving of the direction, they continue to apply in relation to it with the modification that the reference in section 58(7)(a) to the provisions of Part 2 is to be read as including a reference to the provisions of this Part.

(7) The Secretary of State may only give a direction under subsection (3) with the approval of a Judicial Commissioner.

(8) In deciding whether to give approval for the purposes of subsection (7), the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(9) Where a Judicial Commissioner refuses to approve a decision by the Secretary of State to give a direction under subsection (3), the Judicial Commissioner must give the Secretary of State written reasons for the decision.

(10) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve such a decision, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision.

(11) A direction under subsection (3)—

(a) may not be revoked;

(b) may be varied but only for the purpose of altering or removing any provision included in the direction under subsection (5).

(12) Subsections (7) to (10) apply in relation to the variation of a direction under subsection (3) as they apply in relation to the giving of a direction under that subsection.

(13) The head of an intelligence service may, at the same time as applying for a direction under subsection (3), apply for a specific BPD warrant under section 205 (and the Secretary of State may issue such a warrant at the same time as giving the direction).

(14) In this section, "associated regulatory provision", in relation to a power of an intelligence service to retain or examine a bulk personal dataset, means any provision which—

(a) is made by or for the purposes of this Act (other than this Part), and

(b) applied in relation to the retention, examination, disclosure or other use of the bulk personal dataset immediately before the giving of a direction under subsection (3).

226 Part 7: interpretation

(1) In this Part—

"class BPD warrant" has the meaning given by section 200(3)(a);

"personal data" has the meaning given by section 199(2);

"senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

"specific BPD warrant" has the meaning given by section 200(3)(b);

"the specified operational purposes" has the meaning given by section 212(12).

(2) See also—

section 263 (general definitions),

section 265 (index of defined expressions).

PART 8

OVERSIGHT ARRANGEMENTS

CHAPTER 1

INVESTIGATORY POWERS COMMISSIONER AND OTHER JUDICIAL COMMISSIONERS

The Commissioners

227 Investigatory Powers Commissioner and other Judicial Commissioners

(1) The Prime Minister must appoint—

(a) the Investigatory Powers Commissioner, and

(b) such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners.

(2) A person is not to be appointed as the Investigatory Powers Commissioner or another Judicial Commissioner unless the person holds or has held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005).

(3) A person is not to be appointed as the Investigatory Powers Commissioner unless recommended jointly by—

(a) the Lord Chancellor,

(b) the Lord Chief Justice of England and Wales,

(c) the Lord President of the Court of Session, and

(d) the Lord Chief Justice of Northern Ireland.

(4) A person is not to be appointed as a Judicial Commissioner under subsection (1)(b) unless recommended jointly by—

(a) the Lord Chancellor,

(b) the Lord Chief Justice of England and Wales,

(c) the Lord President of the Court of Session,

(d) the Lord Chief Justice of Northern Ireland, and

(e) the Investigatory Powers Commissioner.

(5) Before appointing any person under subsection (1), the Prime Minister must consult the Scottish Ministers.

(6) The Prime Minister must have regard to a memorandum of understanding agreed between the Prime Minister and the Scottish Ministers when exercising functions under subsection (1) or (5).

(7) The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners.

(8) The Investigatory Powers Commissioner may, to such extent as the Investigatory Powers Commissioner may decide, delegate the exercise of functions of the Investigatory Powers Commissioner to any other Judicial Commissioner.

(9) Subsection (8) does not apply to the function of the Investigatory Powers Commissioner of making a recommendation under subsection (4)(e) or making an appointment under section 247(1).

(10) The delegation under subsection (8) to any extent of functions by the Investigatory Powers Commissioner does not prevent the exercise of the functions to that extent by that Commissioner.

(11) Any function exercisable by a Judicial Commissioner or any description of Judicial Commissioners is exercisable by any of the Judicial Commissioners or (as the case may be) any of the Judicial Commissioners of that description.

(12) Subsection (11) does not apply to—

(a) any function conferred on the Investigatory Powers Commissioner by name (except so far as its exercise by any of the Judicial Commissioners or any description of Judicial Commissioners is permitted by a delegation under subsection (8)), or

(b) any function conferred on, or delegated under subsection (8) to, any other particular named Judicial Commissioner.

(13) References in any enactment—

(a) to a Judicial Commissioner are to be read as including the Investigatory Powers Commissioner, and

(b) to the Investigatory Powers Commissioner are to be read, so far as necessary for the purposes of subsection (8), as references to the Investigatory Powers Commissioner or any other Judicial Commissioner.

228 Terms and conditions of appointment

(1) Subject as follows, each Judicial Commissioner holds and vacates office in accordance with the Commissioner's terms and conditions of appointment.

(2) Each Judicial Commissioner is to be appointed for a term of three years.

(3) A person who ceases to be a Judicial Commissioner (otherwise than under subsection (5)) may be re-appointed under section 227(1).

(4) A Judicial Commissioner may not, subject to subsection (5), be removed from office before the end of the term for which the Commissioner is appointed unless a resolution approving the removal has been passed by each House of Parliament.

(5) A Judicial Commissioner may be removed from office by the Prime Minister if, after the appointment of the Commissioner—

(a) a bankruptcy order is made against the Commissioner or the Commissioner's estate is sequestrated or the Commissioner makes a composition or arrangement with, or grants a trust deed for, the Commissioner's creditors,

(b) any of the following orders is made against the Commissioner—

(i) a disqualification order under the Company Directors Disqualification Act 1986 or the Company Directors Disqualification (Northern Ireland) Order 2002,

(ii) an order under section 429(2)(b) of the Insolvency Act 1986 (failure to pay under county court administration order),

(iii) an order under section 429(2) of the Insolvency Act 1986 (disabilities on revocation of county court administration order),

(c) the Commissioner's disqualification undertaking is accepted under section 7 or 8 of the Company Directors Disqualification Act 1986 or under the Company Directors Disqualification (Northern Ireland) Order 2002, or

(d) the Commissioner is convicted in the United Kingdom, the Channel Islands or the Isle of Man of an offence and receives a sentence of imprisonment (whether suspended or not).

Main functions of Commissioners

229 Main oversight functions

(1) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to—

(a) the interception of communications,

(b) the acquisition or retention of communications data,

(c) the acquisition of secondary data or related systems data under Chapter 1 of Part 2 or Chapter 1 of Part 6, or

(d) equipment interference.

(2) Such statutory functions include, in particular, functions relating to the disclosure, retention or other use of—

(a) any content of communications intercepted by an interception authorised or required by a warrant under Chapter 1 of Part 2 or Chapter 1 of Part 6,

(b) acquired or retained communications data,

(c) data acquired as mentioned in subsection (1)(c), or

(d) communications, equipment data or other information acquired by means of equipment interference.

(3) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation)—

(a) the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service,

(b) the giving and operation of notices under section 252 (national security notices),

(c) the exercise of functions by virtue of section 80 of the Serious Crime Act 2015 (prevention or restriction of use of communication devices by prisoners etc.),

(d) the exercise of functions by virtue of sections 1 to 4 of the Prisons (Interference with Wireless Telegraphy) Act 2012,

(e) the exercise of functions by virtue of Part 2 or 3 of the Regulation of Investigatory Powers Act 2000 (surveillance, covert human intelligence sources and investigation of electronic data protected by encryption etc.),

(f) the adequacy of the arrangements by virtue of which the duties imposed by section 55 of that Act are sought to be discharged,

(g) the exercise of functions by virtue of the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11) (surveillance and covert human intelligence sources),

(h) the exercise of functions under Part 3 of the Police Act 1997 (authorisation of action in respect of property),

(i) the exercise by the Secretary of State of functions under sections 5 to 7 of the Intelligence Services Act 1994 (warrants for interference with wireless telegraphy, entry and interference with property etc.), and

(j) the exercise by the Scottish Ministers (by virtue of provision made under section 63 of the Scotland Act 1998) of functions under sections 5 and 6(3) and (4) of the Act of 1994.

(4) But the Investigatory Powers Commissioner is not to keep under review—

(a) the exercise of any function of a relevant Minister to make subordinate legislation,

(b) the exercise of any function by a judicial authority,

(c) the exercise of any function by virtue of Part 3 of the Regulation of Investigatory Powers Act 2000 which is exercisable with the permission of a judicial authority,

(d) the exercise of any function which—

(i) is for the purpose of obtaining information or taking possession of any document or other property in connection with communications stored in or by a telecommunication system, or

(ii) is carried out in accordance with an order made by a judicial authority for that purpose,

and is not exercisable by virtue of this Act, the Regulation of Investigatory Powers Act 2000, the Regulation of Investigatory Powers (Scotland) Act 2000 or an enactment mentioned in subsection (3)(c), (h), (i) or (j) above,

(e) the exercise of any function where the conduct concerned is—

(i) conduct authorised by section 45, 47 or 50, or

(ii) conduct authorised by section 46 which is not conduct by or on behalf of an intercepting authority (within the meaning given by section 18(1)), or

(f) the exercise of any function which is subject to review by the Information Commissioner or the Investigatory Powers Commissioner for Northern Ireland.

(5) In keeping matters under review in accordance with this section, the Investigatory Powers Commissioner must, in particular, keep under review the operation of safeguards to protect privacy.

(6) In exercising functions under this Act, a Judicial Commissioner must not act in a way which the Commissioner considers to be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime, or

(c) the economic well-being of the United Kingdom.

(7) A Judicial Commissioner must, in particular, ensure that the Commissioner does not—

(a) jeopardise the success of an intelligence or security operation or a law enforcement operation,

(b) compromise the safety or security of those involved, or

(c) unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces.

(8) Subsections (6) and (7) do not apply in relation to any of the following functions of a Judicial Commissioner—

(a) deciding—

(i) whether to serve, vary or cancel a monetary penalty notice under section 7 or paragraph 16 of Schedule 1, a notice of intent under paragraph 4 of that Schedule or an information notice under Part 2 of that Schedule, or

(ii) the contents of any such notice,

(b) deciding whether to approve the issue, modification or renewal of a warrant,

(c) deciding whether to direct the destruction of material or how otherwise to deal with the situation where—

(i) a warrant issued, or modification made, for what was considered to be an urgent need is not approved, or

(ii) an item subject to legal privilege is retained, following its examination, for purposes other than the destruction of the item,

(d) deciding whether to—

(i) approve the grant, modification or renewal of an authorisation, or

(ii) quash or cancel an authorisation or renewal,

(e) deciding whether to approve—

(i) the giving or varying of a retention notice under Part 4 or a notice under section 252 or 253, or

(ii) the giving of a notice under section 90(10)(b) or 257(9)(b),

(f) participating in a review under section 90 or 257,

(g) deciding whether to approve an authorisation under section 219(3)(b),

(h) deciding whether to give approval under section 222(4),

(i) deciding whether to approve the giving or varying of a direction under section 225(3),

(j) making a decision under section 231(1),

(k) deciding whether to order the destruction of records under section 103 of the Police Act 1997, section 37 of the Regulation of Investigatory Powers Act 2000 or section 15 of the Regulation of Investigatory Powers (Scotland) Act 2000,

(l) deciding whether to make an order under section 103(6) of the Police Act 1997 (order enabling the taking of action to retrieve anything left on property in pursuance of an authorisation),

(m) deciding—

(i) an appeal against, or a review of, a decision by another Judicial Commissioner, and

(ii) any action to take as a result.

(9) In this section—

"bulk personal dataset" is to be read in accordance with section 199,

"equipment data" has the same meaning as in Part 5 (see section 100),

"judicial authority" means a judge, court or tribunal or any person exercising the functions of a judge, court or tribunal (but does not include a Judicial Commissioner),

"police force" has the same meaning as in Part 2 (see section 60(1)),

"related systems data" has the meaning given by section 15(6),

"relevant Minister" means a Minister of the Crown or government department, the Scottish Ministers, the Welsh Ministers or a Northern Ireland department,

"secondary data" has the same meaning as in Part 2 (see section 16).

230 Additional directed oversight functions

(1) So far as directed to do so by the Prime Minister and subject to subsection (2), the Investigatory Powers Commissioner must keep under review the carrying out of any aspect of the functions of—

(a) an intelligence service,

(b) a head of an intelligence service, or

(c) any part of Her Majesty's forces, or of the Ministry of Defence, so far as engaging in intelligence activities.

(2) Subsection (1) does not apply in relation to anything which is required to be kept under review by the Investigatory Powers Commissioner under section 229.

(3) The Prime Minister may give a direction under this section at the request of the Investigatory Powers Commissioner or the Intelligence and Security Committee of Parliament or otherwise.

(4) The Prime Minister must publish, in a manner which the Prime Minister considers appropriate, any direction under this section (and any revocation of such a direction) except so far as it appears to the Prime Minister that such publication would be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime,

(c) the economic well-being of the United Kingdom, or

(d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

231 Error reporting

(1) The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person of which the Commissioner is aware if the Commissioner considers that—

(a) the error is a serious error, and

(b) it is in the public interest for the person to be informed of the error.

(2) In making a decision under subsection (1)(a), the Investigatory Powers Commissioner may not decide that an error is a serious error unless the Commissioner considers that the error has caused significant prejudice or harm to the person concerned.

(3) Accordingly, the fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

(4) In making a decision under subsection (1)(b), the Investigatory Powers Commissioner must, in particular, consider—

(a) the seriousness of the error and its effect on the person concerned, and

(b) the extent to which disclosing the error would be contrary to the public interest or prejudicial to—

(i) national security,

(ii) the prevention or detection of serious crime,

(iii) the economic well-being of the United Kingdom, or

(iv) the continued discharge of the functions of any of the intelligence services.

(5) Before making a decision under subsection (1)(a) or (b), the Investigatory Powers Commissioner must ask the public authority which has made the error to make submissions to the Commissioner about the matters concerned.

(6) When informing a person under subsection (1) of an error, the Investigatory Powers Commissioner must—

(a) inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and

(b) provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights, having regard in particular to the extent to which disclosing the details would be contrary to the public interest or prejudicial to anything falling within subsection (4)(b)(i) to (iv).

(7) The Investigatory Powers Commissioner may not inform the person to whom it relates of a relevant error except as provided by this section.

(8) A report under section 234(1) must include information about—

(a) the number of relevant errors of which the Investigatory Powers Commissioner has become aware during the year to which the report relates,

(b) the number of relevant errors which the Commissioner has decided during that year were serious errors, and

(c) the number of persons informed under subsection (1) during that year.

(9) In this section "relevant error" means an error—

(a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and

(b) of a description identified for this purpose in a code of practice under Schedule 7,

and the Investigatory Powers Commissioner must keep under review the definition of "relevant error".

232 Additional functions under this Part

(1) A Judicial Commissioner must give the Investigatory Powers Tribunal all such documents, information and other assistance (including the Commissioner's opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require—

(a) in connection with the investigation of any matter by the Tribunal, or

(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter.

(2) A Judicial Commissioner may provide advice or information to any public authority or other person in relation to matters for which a Judicial Commissioner is responsible.

(3) But a Judicial Commissioner must consult the Secretary of State before providing any advice or information under subsection (2) if it appears to the Commissioner that providing the advice or information might be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime,

(c) the economic well-being of the United Kingdom, or

(d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

(4) In addition to consulting the Secretary of State under subsection (3), the Judicial Commissioner must also consult the Scottish Ministers if it appears to the Commissioner that providing the advice or information might be prejudicial to—

(a) the prevention or detection of serious crime by a Scottish public authority, or

(b) the continued discharge of any devolved functions of a Scottish public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

(5) In subsection (4)—

"devolved function" means a function that does not relate to reserved matters (within the meaning of the Scotland Act 1998), and

"Scottish public authority" has the same meaning as in the Scotland Act 1998.

(6) Subsections (3) and (4) do not apply to any advice or information provided under subsection (2) to the Investigatory Powers Tribunal.

233 Functions under other Parts and other enactments

(1) The Investigatory Powers Commissioner and the other Judicial Commissioners have the functions that are exercisable by them by virtue of any other Part of this Act or by virtue of any other enactment.

(2) In Part 3 of the Police Act 1997 (authorisations of action in respect of property: approval by Commissioners)—

(a) in sections 96(1), 103(7)(b) and (8), 104(3) to (8) and 105(1) and (2) for "Chief Commissioner" substitute "Investigatory Powers Commissioner",

(b) in sections 96(1), 97(1)(a) and 103(1), (2), (4) and (5)(b) for "a Commissioner appointed under section 91(1)(b)" substitute "a Judicial Commissioner",

(c) in sections 96(4), 97(4) and (6) and 103(3) and (6) for "a Commissioner" substitute "a Judicial Commissioner",

(d) in section 103(7) for "a Commissioner" substitute "a Judicial Commissioner (other than the Investigatory Powers Commissioner)",

(e) in section 104(1) for "Chief Commissioner" substitute "Investigatory Powers Commissioner (except where the original decision was made by that Commissioner)",

(f) in section 104(3) and (8)(a) for "the Commissioner" substitute "the Judicial Commissioner concerned",

(g) in section 105(1)(a)(ii) and (b)(ii) for "the Commissioner" substitute "the Judicial Commissioner", and

(h) in sections 97(5) and 103(9) for "A Commissioner" substitute "A Judicial Commissioner".

(3) In Part 2 of the Regulation of Investigatory Powers Act 2000 (surveillance and covert human intelligence sources: approval by Commissioners)—

(a) in sections 35(1) and (4), 36(2)(a) and (5) and 37(2) to (6) and (8) for "an ordinary Surveillance Commissioner", wherever it appears, substitute "a Judicial Commissioner",

(b) in sections 35(2)(b), 36(6)(g), 37(9)(b), 38(1) and (4) to (6) and 39(1), (2) and (4) and in the heading of section 39 for "Chief Surveillance Commissioner", wherever it appears, substitute "Investigatory Powers Commissioner",

(c) in sections 35(3)(a) and 36(4)(a) and (b) for "Surveillance Commissioner" substitute "Judicial Commissioner",

(d) in section 37(8)(b) for "Chief Surveillance Commissioner" substitute "Investigatory Powers Commissioner (if he is not that Commissioner)",

(e) in section 38(1)(a) for "an ordinary Surveillance Commissioner" substitute "a Judicial Commissioner (other than the Investigatory Powers Commissioner)",

(f) in sections 38(5)(b) and 39(1)(b) for "ordinary Surveillance Commissioner" substitute "Judicial Commissioner", and

(g) in the heading of section 38 for "Surveillance Commissioners" substitute "Judicial Commissioners".

(4) In Part 3 of the Act of 2000 (investigation of electronic data protected by encryption etc.)—

(a) in section 51(6) (notification to Intelligence Services Commissioner or Chief Surveillance Commissioner of certain directions relating to the disclosure of a key to protected information) for the words from "done so" to the end substitute "done so to the Investigatory Powers Commissioner",

(b) in section 54(9) (tipping-off: protected disclosures to a relevant Commissioner) for "relevant Commissioner" substitute "Judicial Commissioner",

(c) in section 55(7) (court to have regard to opinion of a relevant Commissioner in certain circumstances relating to a disclosed key) for "relevant Commissioner" substitute "Judicial Commissioner or the Investigatory Powers Commissioner for Northern Ireland", and

(d) omit sections 54(11) and 55(8) (definitions of "relevant Commissioner").

(5) In the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11) (surveillance and covert human intelligence sources: approval by Commissioners and review by the Chief Commissioner)—

(a) in sections 13(1) and (4), 14(1)(a) and (4) and 15(1) to (5) and (7) for "an ordinary Surveillance Commissioner", wherever it appears, substitute "a Judicial Commissioner",

(b) in sections 13(2)(b), 15(8)(b), 16(1) and (4) to (6) and 17 and in the heading of section 17 for "Chief Surveillance Commissioner", wherever it appears, substitute "Investigatory Powers Commissioner",

(c) in sections 13(3)(a) and 14(3)(a) and (b) for "Surveillance Commissioner" substitute "Judicial Commissioner",

(d) in section 15(7)(b) for "Chief Surveillance Commissioner" substitute "Investigatory Powers Commissioner (if the Commissioner is not that Commissioner)",

(e) in section 16(1)(a) for "an ordinary Surveillance Commissioner" substitute "a Judicial Commissioner (other than the Investigatory Powers Commissioner)",

(f) in sections 16(5)(b) and 17(1)(b) for "ordinary Surveillance Commissioner" substitute "Judicial Commissioner", and

(g) in section 16(5) for "ordinary Surveillance Commissioner's" substitute "Judicial Commissioner's".

(6) In Part 2 of the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 (S.I. 2013/2788) (notification of certain authorisations to, and approval of certain authorisations by, ordinary Surveillance Commissioner)—

(a) in article 4(1), for "an ordinary Surveillance Commissioner" substitute "a Judicial Commissioner",

(b) in article 5(8) and the heading of Part 2, for "ordinary Surveillance Commissioner" substitute "Judicial Commissioner",

(c) in article 6(1) and (3) for "Chief Surveillance Commissioner" substitute "Investigatory Powers Commissioner",

(d) in article 6(1) for "an ordinary Surveillance Commissioner" substitute "a Judicial Commissioner (other than the Investigatory Powers Commissioner)", and

(e) in the heading of article 6 for "Surveillance Commissioners" substitute "Judicial Commissioners".

Reports and investigation and information powers

234 Annual and other reports

(1) The Investigatory Powers Commissioner must, as soon as reasonably practicable after the end of each calendar year, make a report to the Prime Minister about the carrying out of the functions of the Judicial Commissioners.

(2) A report under subsection (1) must, in particular, include—

(a) statistics on the use of the investigatory powers which are subject to review by the Investigatory Powers Commissioner (including the number of warrants or authorisations issued, given, considered or approved during the year),

(b) information about the results of such use (including its impact),

(c) information about the operation of the safeguards conferred by this Act in relation to items subject to legal privilege, confidential journalistic material and sources of journalistic information,

(d) information about the following kinds of warrants issued, considered or approved during the year—

(i) targeted interception warrants or targeted examination warrants of the kind referred to in section 17(2),

(ii) targeted equipment interference warrants relating to matters within paragraph (b), (c), (e), (f), (g) or (h) of section 101(1), and

(iii) targeted examination warrants under Part 5 relating to matters within any of paragraphs (b) to (e) of section 101(2),

(e) information about the operational purposes specified during the year in warrants issued under Part 6 or 7,

(f) the information on errors required by virtue of section 231(8),

(g) information about the work of the Technology Advisory Panel,

(h) information about the funding, staffing and other resources of the Judicial Commissioners, and

(i) details of public engagements undertaken by the Judicial Commissioners or their staff.

(3) The Investigatory Powers Commissioner must, at any time, make any report to the Prime Minister which has been requested by the Prime Minister.

(4) The Investigatory Powers Commissioner may, at any time, make any such report to the Prime Minister, on any matter relating to the functions of the Judicial Commissioners, as the Investigatory Powers Commissioner considers appropriate.

(5) A report under subsection (1) or (4) may, in particular, include such recommendations as the Investigatory Powers Commissioner considers appropriate about any matter relating to the functions of the Judicial Commissioners.

(6) On receiving a report from the Investigatory Powers Commissioner under subsection (1), the Prime Minister must—

(a) publish the report, and

(b) lay a copy of the published report before Parliament together with a statement as to whether any part of the report has been excluded from publication under subsection (7).

(7) The Prime Minister may, after consultation with the Investigatory Powers Commissioner and (so far as the report relates to functions under Part 3 of the Police Act 1997) the Scottish Ministers, exclude from publication any part of a report under subsection (1) if, in the opinion of the Prime Minister, the publication of that part would be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime,

(c) the economic well-being of the United Kingdom, or

(d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

(8) The Prime Minister must send a copy of every report and statement as laid before Parliament under subsection (6)(b) to the Scottish Ministers and the Scottish Ministers must lay the copy report and statement before the Scottish Parliament.

(9) The Investigatory Powers Commissioner may publish any report under subsection (3) or (4), or any part of such a report, if requested to do so by the Prime Minister.

(10) Subsection (11) applies if the Prime Minister receives a report from the Investigatory Powers Commissioner under subsection (1) or (4) which relates to an investigation, inspection or audit carried out by the Commissioner following a decision to do so of which the Intelligence and Security Committee of Parliament was informed under section 236(2).

(11) The Prime Minister must send to the Intelligence and Security Committee of Parliament a copy of the report so far as it relates to—

(a) the investigation, inspection or audit concerned, and

(b) the functions of the Committee falling within section 2 of the Justice and Security Act 2013.

235 Investigation and information powers

(1) A Judicial Commissioner may carry out such investigations, inspections and audits as the Commissioner considers appropriate for the purposes of the Commissioner's functions.

(2) Every relevant person must disclose or provide to a Judicial Commissioner all such documents and information as the Commissioner may require for the purposes of the Commissioner's functions.

(3) Every relevant person must provide a Judicial Commissioner with such assistance as the Commissioner may require in carrying out any investigation, inspection or audit for the purposes of the Commissioner's functions.

(4) Assistance under subsection (3) may, in particular, include such access to apparatus, systems or other facilities or services as the Judicial Commissioner concerned may require in carrying out any investigation, inspection or audit for the purposes of the Commissioner's functions.

(5) A public authority may report to the Investigatory Powers Commissioner any refusal by a telecommunications operator or postal operator to comply with any requirements imposed by virtue of this Act.

(6) A public authority, telecommunications operator or postal operator must report to the Investigatory Powers Commissioner any relevant error (within the meaning given by section 231(9)) of which it is aware.

(7) In this section "relevant person" means—

(a) any person who holds, or has held, an office, rank or position with a public authority,

(b) any telecommunications operator or postal operator who is, has been or may become subject to a requirement imposed by virtue of this Act,

(c) any person who is, has been or may become subject to a requirement to provide assistance by virtue of section 41, 43, 126, 128, 149, 168, 170 or 190, or

(d) any person to whom a notice is given under section 49 of the Regulation of Investigatory Powers Act 2000.

236 Referrals by the Intelligence and Security Committee of Parliament

(1) Subsection (2) applies if the Intelligence and Security Committee of Parliament refers a matter to the Investigatory Powers Commissioner with a view to the Commissioner carrying out an investigation, inspection or audit into it.

(2) The Investigatory Powers Commissioner must inform the Intelligence and Security Committee of Parliament of the Commissioner's decision as to whether to carry out the investigation, inspection or audit.

237 Information gateway

(1) A disclosure of information to the Investigatory Powers Commissioner or another Judicial Commissioner for the purposes of any function of the Commissioner does not breach—

(a) an obligation of confidence owed by the person making the disclosure, or

(b) any other restriction on the disclosure of information (whether imposed by virtue of this Act or otherwise).

(2) But subsection (1) does not apply to a disclosure, in contravention of any provisions of the Data Protection Act 1998, of personal data which is not exempt from those provisions.

Supplementary provision

238 Funding, staff and facilities etc.

(1) There is to be paid to the Judicial Commissioners out of money provided by Parliament such remuneration and allowances as the Treasury may determine.

(2) The Secretary of State must, after consultation with the Investigatory Powers Commissioner and subject to the approval of the Treasury as to numbers of staff, provide the Judicial Commissioners with—

(a) such staff, and

(b) such accommodation, equipment and other facilities and services,

as the Secretary of State considers necessary for the carrying out of the Commissioners' functions.

(3) The Scottish Ministers may pay to the Judicial Commissioners such allowances as the Scottish Ministers consider appropriate in respect of the exercise by the Commissioners of functions which relate to the exercise by Scottish public authorities of devolved functions.

(4) In subsection (3)—

"devolved function" means a function that does not relate to reserved matters (within the meaning of the Scotland Act 1998), and

"Scottish public authority" has the same meaning as in the Scotland Act 1998.

(5) The Investigatory Powers Commissioner or any other Judicial Commissioner may, to such extent as the Commissioner concerned may decide, delegate the exercise of functions of that Commissioner to any member of staff of the Judicial Commissioners or any other person acting on behalf of the Commissioners.

(6) Subsection (5) does not apply to—

(a) the function of the Investigatory Powers Commissioner of making a recommendation under section 227(4)(e) or making an appointment under section 247(1),

(b) any function which falls within section 229(8), or

(c) any function under section 58(4) or 133(3) of authorising a disclosure,

but, subject to this and the terms of the delegation, does include functions which have been delegated to a Judicial Commissioner by the Investigatory Powers Commissioner.

(7) The delegation under subsection (5) to any extent of functions by the Investigatory Powers Commissioner or any other Judicial Commissioner does not prevent the exercise of the functions to that extent by the Commissioner concerned.

239 Power to modify functions

(1) The Secretary of State may by regulations modify the functions of the Investigatory Powers Commissioner or any other Judicial Commissioner.

(2) But such regulations may not modify any function conferred by virtue of this Act on a Judicial Commissioner to approve, quash or cancel—

(a) an authorisation or warrant, or

(b) the variation or renewal of an authorisation or warrant.

(3) The power to make regulations under this section (including that power as extended by section 267(1)(c)) may, in particular, be exercised by modifying any provision made by or under an enactment (including this Act).

240 Abolition of existing oversight bodies

(1) The offices of the following are abolished—

(a) the Interception of Communications Commissioner,

(b) the Intelligence Services Commissioner,

(c) the Chief Surveillance Commissioner,

(d) the other Surveillance Commissioners,

(e) the Scottish Chief Surveillance Commissioner, and

(f) the other Scottish Surveillance Commissioners.

(2) Accordingly, the following enactments are repealed—

(a) sections 57 and 58 of the Regulation of Investigatory Powers Act 2000 (the Interception of Communications Commissioner),

(b) sections 59, 59A and 60 of that Act (the Intelligence Services Commissioner),

(c) sections 62 and 63 of that Act and sections 91 and 107 of the Police Act 1997 (the Surveillance Commissioners), and

(d) sections 2(1) to (9), 3 and 4 of the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11) (the Scottish Surveillance Commissioners).

(3) The Secretary of State may by regulations, with the consent of the Northern Ireland Assembly, provide for the abolition of the office of the Investigatory Powers Commissioner for Northern Ireland.

(4) The power to make regulations under subsection (3) (including that power as extended by section 267(1)(c)) may, in particular, be exercised by modifying any provision made by or under an enactment (including this Act).

(5) Regulations made by virtue of subsection (4) may, in particular, repeal—

(a) section 61 of the Regulation of Investigatory Powers Act 2000 (the Investigatory Powers Commissioner for Northern Ireland), and

(b) the words "or the Investigatory Powers Commissioner for Northern Ireland" in section 229(4)(f) of this Act.

(6) In this section—

"the Chief Surveillance Commissioner" means the Chief Commissioner appointed under section 91(1)(a) of the Police Act 1997,

"the other Scottish Surveillance Commissioners" means—

(a) the Surveillance Commissioners appointed under section 2(1)(b) of the Regulation of Investigatory Powers (Scotland) Act 2000, and

(b) the Assistant Surveillance Commissioners appointed under section 3 of that Act,

"the other Surveillance Commissioners" means—

(a) the Commissioners appointed under section 91(1)(b) of the Police Act 1997, and

(b) the Assistant Surveillance Commissioners appointed under section 63(1) of the Regulation of Investigatory Powers Act 2000,

"the Scottish Chief Surveillance Commissioner" means the Chief Surveillance Commissioner appointed under section 2(1)(a) of the Regulation of Investigatory Powers (Scotland) Act 2000.

CHAPTER 2

OTHER ARRANGEMENTS

Codes of practice

241 Codes of practice

Schedule 7 (codes of practice) has effect.

Investigatory Powers Tribunal

242 Right of appeal from Tribunal

(1) After section 67 of the Regulation of Investigatory Powers Act 2000 insert—

"**67A Appeals from the Tribunal**

(1) A relevant person may appeal on a point of law against any determination of the Tribunal of a kind mentioned in section 68(4) or any decision of the Tribunal of a kind mentioned in section 68(4C).

(2) Before making a determination or decision which might be the subject of an appeal under this section, the Tribunal must specify the court which is to have jurisdiction to hear the appeal (the "relevant appellate court").

(3) This court is whichever of the following courts appears to the Tribunal to be the most appropriate—

(a) the Court of Appeal in England and Wales,

(b) the Court of Session.

(4) The Secretary of State may by regulations, with the consent of the Northern Ireland Assembly, amend subsection (3) so as to add the Court of Appeal in Northern Ireland to the list of courts mentioned there.

(5) The Secretary of State may by regulations specify criteria to be applied by the Tribunal in making decisions under subsection (2) as to the identity of the relevant appellate court.

(6) An appeal under this section—

(a) is to be heard by the relevant appellate court, but

(b) may not be made without the leave of the Tribunal or, if that is refused, of the relevant appellate court.

(7) The Tribunal or relevant appellate court must not grant leave to appeal unless it considers that—

(a) the appeal would raise an important point of principle or practice, or

(b) there is another compelling reason for granting leave.

(8) In this section—

"relevant appellate court" has the meaning given by subsection (2),

"relevant person", in relation to any proceedings, complaint or reference, means the complainant or—

(a) in the case of proceedings, the respondent,

(b) in the case of a complaint, the person complained against, and

(c) in the case of a reference, any public authority to whom the reference relates."

(2) In section 67 of that Act (no appeal from the Investigatory Powers Tribunal except as provided by order of the Secretary of State)—

(a) in subsection (8) for "Except to such extent as the Secretary of State may by order otherwise provide," substitute "Except as provided by virtue of section 67A,", and

(b) omit subsections (9) to (12).

(3) After section 68(4) of that Act (requirement to give notice of determinations to complainant) insert—

"(4A) Where the Tribunal make any determination of a kind mentioned in subsection (4), they must also give notice to—

(a) in the case of proceedings, the respondent,

(b) in the case of a complaint, the person complained against, and

(c) in the case of a reference, any public authority to whom the reference relates.

(4B) A notice under subsection (4A) is (subject to any rules made by virtue of section 69(2)(j)) to be confined, as the case may be, to either—

(a) a statement that they have made a determination in the complainant's favour, or

(b) a statement that no determination has been made in the complainant's favour.

(4C) Where the Tribunal make any decision which—

(a) is a final decision of a preliminary issue in relation to any proceedings, complaint or reference brought before or made to them, and

(b) is neither a determination of a kind mentioned in subsection (4) nor a decision relating to a procedural matter,

they must give notice of that decision to every person who would be entitled to receive notice of the determination under subsection (4) or (4A).

(4D) A notice under subsection (4C) is (subject to any rules made by virtue of section 69(2)(i) or (j)) to be confined to a statement as to what the decision is.

(4E) Subsections (4C) and (4D) do not apply so far as—

(a) the Tribunal are prevented from giving notice of a decision to a person by rules made by virtue of section 69(4) or decide under such rules not to give such a notice, or

(b) the giving of such a notice is inconsistent with such rules."

(4) In section 69(2) of that Act (Tribunal rules)—

(a) in paragraph (i), after "section 68(4)" insert "or notice under section 68(4C)", and

(b) after paragraph (i), insert ";

(j) require information about any determination, award, order or other decision made by the Tribunal in relation to any proceedings, complaint or reference to be provided (in addition to any statement under section 68(4A) or notice under section 68(4C)) to—

(i) in the case of proceedings, the respondent,

(ii) in the case of a complaint, the person complained against, and

(iii) in the case of a reference, any public authority to whom the reference relates,

or to the person representing their interests;

(k) make provision about the making and determination of applications to the Tribunal for permission to appeal".

(5) In section 78 of that Act (orders, regulations and rules)—

(a) in subsection (4), after "applies" insert "(other than regulations under section 67A(5))", and

(b) after subsection (4) insert—

"(4A) A statutory instrument containing regulations under section 67A(5) may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament."

243 Functions of Tribunal in relation to this Act etc.

(1) In section 65 of the Regulation of Investigatory Powers Act 2000 (the Investigatory Powers Tribunal)—

(a) in subsection (2)(c) (jurisdiction of the Investigatory Powers Tribunal where possible detriment due to evidential bar) for "section 17" substitute "section 56 of the Investigatory Powers Act 2016",

(b) in subsection (5) (conduct in relation to which the Tribunal has jurisdiction) after paragraph (b) insert—

"(ba) conduct for or in connection with the obtaining of secondary data from communications transmitted by means of such a service or system;

(bb) the issue, modification, renewal or service of a warrant under Part 2 or Chapter 1 of Part 6 of the Investigatory Powers Act 2016 (interception of communications);",

(c) in subsection (5) for paragraph (c) substitute—

"(c) conduct of a kind which may be permitted or required by an authorisation or notice under Part 3 of that Act or a warrant under Chapter 2 of Part 6 of that Act (acquisition of communications data);

(cza) the giving of an authorisation or notice under Part 3 of that Act or the issue, modification, renewal or service of a warrant under Chapter 2 of Part 6 of that Act;

(czb) conduct of a kind which may be required or permitted by a retention notice under Part 4 of that Act (retention of communications data) but excluding any conduct which is subject to review by the Information Commissioner;

(czc) the giving or varying of a retention notice under that Part of that Act;

(czd) conduct of a kind which may be required or permitted by a warrant under Part 5 or Chapter 3 of Part 6 of that Act (equipment interference);

(cze) the issue, modification, renewal or service of a warrant under Part 5 or Chapter 3 of Part 6 of that Act;

(czf) the issue, modification, renewal or service of a warrant under Part 7 of that Act (bulk personal dataset warrants);

(czg) the giving of an authorisation under section 219(3)(b) (authorisation for the retention, or retention and examination, of material following expiry of bulk personal dataset warrant);

(czh) the giving or varying of a direction under section 225 of that Act (directions where no bulk personal dataset warrant required);

(czi) conduct of a kind which may be required by a notice under section 252 or 253 of that Act (national security or technical capability notices);

(czj) the giving or varying of such a notice;

(czk) the giving of an authorisation under section 152(5)(c) or 193(5)(c) of that Act (certain authorisations to examine intercepted content or protected material);

(czl) any failure to—

(i) cancel a warrant under Part 2, 5, 6 or 7 of that Act or an authorisation under Part 3 of that Act;

(ii) cancel a notice under Part 3 of that Act;

(iii) revoke a notice under Part 4, or section 252 or 253, of that Act; or

(iv) revoke a direction under section 225 of that Act;

(czm) any conduct in connection with any conduct falling within paragraph (c), (czb), (czd) or (czi);",

(d) in subsection (6) (limitation for certain purposes of what is conduct falling within subsection (5))—

(i) after "on behalf of" insert "an immigration officer or", and

(ii) after paragraph (d) insert—

"(dza) the Competition and Markets Authority;",

(e) after subsection (6) insert—

"(6A) Subsection (6) does not apply to anything mentioned in paragraph (d) or (f) of subsection (5) which also falls within paragraph (czd) of that subsection.",

(f) in subsection (7) after "if" insert "it is conduct of a public authority and",

(g) in subsection (7ZA) (role for Tribunal where judicial authority involved) for "under section 23A or 32A" substitute "by a Judicial Commissioner or under section 32A of this Act or section 75 of the Investigatory Powers Act 2016",

(h) after subsection (7ZA) insert—

"(7ZB) For the purposes of this section conduct also takes place in challengeable circumstances if it is, or purports to be, conduct falling within subsection (5)(bb), (cza), (czc), (cze), (czf), (czg), (czh), (czj), (czk) or (czl) or (so far as the conduct is, or purports to be, the giving of a notice under section 49) subsection (5)(e).",

(i) in subsection (8) (matters that may be challenged before the Tribunal) for paragraphs (a) and (b) substitute—

"(a) a warrant under Part 2, 5, 6 or 7 of the Investigatory Powers Act 2016;

(b) an authorisation or notice under Part 3 of that Act;

(ba) a retention notice under Part 4 of that Act;

(bb) a direction under section 225 of that Act;

(bc) a notice under section 252 or 253 of that Act;", and

(j) after subsection (9) insert—

"(9A) In subsection (5)(ba) the reference to obtaining secondary data from communications transmitted by means of a postal service or telecommunication system is to be read in accordance with section 16 of the Investigatory Powers Act 2016."

(2) In section 67(7) of the Act of 2000 (powers of the Tribunal)—

(a) after paragraph (a) insert—

"(aza) an order quashing or cancelling a notice under Part 3 of the Investigatory Powers Act 2016 or a retention notice under Part 4 of that Act;

(azb) an order quashing or revoking a direction under section 225 of that Act;

(azc) an order quashing or revoking a notice under section 252 or 253 of that Act;",

(b) in paragraph (aa) for "section 23A or 32A" substitute "section 75 of the Investigatory Powers Act 2016 or section 32A of this Act", and

(c) in paragraph (b)(i) after "authorisation" insert "or by a notice under Part 3 of the Investigatory Powers Act 2016".

(3) In section 68(5)(b) of the Act of 2000 (report of certain findings to the Prime Minister) after "permission" insert ", or notice under Part 4 of the Investigatory Powers Act 2016 or under section 252 or 253 of that Act or direction under section 225 of that Act,".

(4) In section 68(6)(b) of the Act of 2000 (disclosures etc. to the Tribunal to enable the exercise of functions conferred by or under that Act) after "this Act" insert "or the Investigatory Powers Act 2016".

(5) In section 68(7) of the Act of 2000 (persons subject to duty to co-operate with the Tribunal)—

(a) in paragraph (e)—

(i) for "section 11" substitute "section 41, 126, 149, 168 or 190 of the Investigatory Powers Act 2016", and

(ii) for "an interception warrant" substitute "a warrant",

(b) in paragraph (f) for "section 12" substitute "section 252 or 253 of that Act",

(c) for paragraphs (g) and (h) substitute—

"(g) every person by or to whom an authorisation under Part 3 of that Act has been granted;

(h) every person to whom a notice under Part 3 of that Act has been given;

(ha) every person to whom a retention notice under Part 4 of that Act or a notice under section 252 or 253 of that Act has been given;",

(d) in paragraph (k), for the words from "an authorisation" to the end substitute "—

(i) an authorisation under Part 3 of the Investigatory Powers Act 2016, Part 2 of this Act or Part 3 of the Police Act 1997, or

(ii) a warrant under Chapter 2 of Part 6 of the Investigatory Powers Act 2016;",

(e) in paragraph (l) after "authorisation" insert "or warrant", and

(f) in paragraph (n) after "(h)" insert ", (ha)".

(6) In section 68(8) of the Act of 2000 (meaning of "relevant Commissioner") for the words from "Interception" to the end substitute "Investigatory Powers Commissioner or any other Judicial Commissioner or the Investigatory Powers Commissioner for Northern Ireland".

Information Commissioner

244 Oversight by Information Commissioner in relation to Part 4

The Information Commissioner must audit compliance with requirements or restrictions imposed by virtue of Part 4 in relation to the integrity, security or destruction of data retained by virtue of that Part.

Advisory bodies

245 Technical Advisory Board

(1) There is to continue to be a Technical Advisory Board consisting of such number of persons appointed by the Secretary of State as the Secretary of State may by regulations provide.

(2) The regulations providing for the membership of the Technical Advisory Board must also make provision which is calculated to ensure—

(a) that the membership of the Board includes persons likely effectively to represent the interests of persons on whom obligations may be imposed by virtue of retention notices under Part 4, national security notices under section 252 or technical capability notices under section 253,

(b) that the membership of the Board includes persons likely effectively to represent the interests of persons entitled to apply for warrants under Part 2, 5, 6 or 7 or authorisations under Part 3,

(c) that such other persons (if any) as the Secretary of State considers appropriate may be appointed to be members of the Board, and

(d) that the Board is so constituted as to produce a balance between the representation of the interests mentioned in paragraph (a) and the representation of those mentioned in paragraph (b).

(3) Regulations under this section may also make provision about quorum and the filling of vacancies.

246 Technology Advisory Panel

(1) The Investigatory Powers Commissioner must ensure that there is a Technology Advisory Panel to provide advice to the Investigatory Powers Commissioner, the Secretary of State and the Scottish Ministers about—

(a) the impact of changing technology on the exercise of investigatory powers whose exercise is subject to review by the Commissioner, and

(b) the availability and development of techniques to use such powers while minimising interference with privacy.

(2) The Technology Advisory Panel must provide advice to the Investigatory Powers Commissioner about such matters falling within subsection (1)(a) or (b) as the Commissioner may direct.

(3) Subject to this, the Panel may provide advice to the Investigatory Powers Commissioner about such matters falling within subsection (1)(a) or (b) as it considers appropriate (whether or not requested to do so).

(4) The Panel may provide advice to the Secretary of State or the Scottish Ministers about such matters falling within subsection (1)(a) or (b) as it considers appropriate (whether or not requested to do so) but such advice to the Scottish Ministers may only relate to matters for which the Scottish Ministers are responsible.

(5) The Panel must, as soon as reasonably practicable after the end of each calendar year, make a report to the Investigatory Powers Commissioner about the carrying out of the functions of the Panel.

(6) The Panel must, at the same time, send a copy of the report to the Secretary of State and (so far as relating to matters for which the Scottish Ministers are responsible) the Scottish Ministers.

247 Members of the Panel

(1) The Investigatory Powers Commissioner must appoint such number of persons as members of the Technology Advisory Panel as the Commissioner considers necessary for the carrying out of the functions of the Panel.

(2) Subject as follows, each member of the Panel holds and vacates office in accordance with the member's terms and conditions of appointment.

(3) A member of the Panel must not act in a way which the member considers to be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime, or

(c) the economic well-being of the United Kingdom.

(4) A member of the Panel must, in particular, ensure that the member does not—

(a) jeopardise the success of an intelligence or security operation or a law enforcement operation,

(b) compromise the safety or security of those involved, or

(c) unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces.

(5) Section 235(2) and (7) (information powers) apply to a member of the Panel as they apply to a Judicial Commissioner.

PART 9

MISCELLANEOUS AND GENERAL PROVISIONS

CHAPTER 1

MISCELLANEOUS

Combined warrants and authorisations

248 Combination of warrants and authorisations

Schedule 8 (which makes provision for the combination of certain warrants and authorisations in a single instrument) has effect.

Compliance with Act

249 Payments towards certain compliance costs

(1) The Secretary of State must ensure that arrangements are in force for securing that telecommunications operators and postal operators receive an appropriate contribution in respect of such of their relevant costs as the Secretary of State considers appropriate.

(2) In subsection (1) "relevant costs" means costs incurred, or likely to be incurred, by telecommunications operators and postal operators in complying with this Act.

(3) The arrangements may provide for payment of a contribution to be subject to terms and conditions determined by the Secretary of State.

(4) Such terms and conditions may, in particular, include a condition on the operator concerned to comply with any audit that may reasonably be required to monitor the claim for costs.

(5) The arrangements may provide for the Secretary of State to determine—

(a) the scope and extent of the arrangements, and

(b) the appropriate level of contribution which should be made in each case.

(6) Different levels of contribution may apply for different cases or descriptions of case but the appropriate contribution must never be nil.

(7) A retention notice under Part 4 given to a telecommunications operator or a postal operator, or a national security notice under section 252 given to a telecommunications operator, must specify the level or levels of contribution which the Secretary of State has determined should be made in respect of the costs incurred, or likely to be incurred, by the operator as a result of the notice in complying with that Part or (as the case may be) with the national security notice.

(8) For the purpose of complying with this section the Secretary of State may make, or arrange for the making of, payments out of money provided by Parliament.

250 Power to develop compliance systems etc.

(1) The Secretary of State may—

(a) develop, provide, maintain or improve, or

(b) enter into financial or other arrangements with any person for the development, provision, maintenance or improvement of,

such apparatus, systems or other facilities or services as the Secretary of State considers appropriate for enabling or otherwise facilitating compliance by the Secretary of State, another public authority or any other person with this Act.

(2) Arrangements falling within subsection (1)(b) may, in particular, include arrangements consisting of the giving of financial assistance by the Secretary of State.

(3) Such financial assistance—

(a) may, in particular, be given by way of—

(i) grant,

(ii) loan,

(iii) guarantee or indemnity,

(iv) investment, or

(v) incurring expenditure for the benefit of the person assisted, and

(b) may be given subject to terms and conditions determined by the Secretary of State.

(4) Terms and conditions imposed by virtue of subsection (3)(b) may include terms and conditions as to repayment with or without interest.

Additional powers

251 Amendments of the Intelligence Services Act 1994

(1) The Intelligence Services Act 1994 is amended as follows.

(2) In section 3 (the Government Communications Headquarters)—

(a) in subsection (1)(a), after "monitor" insert ", make use of", and

(b) in the words following subsection (1)(b)(ii), for the words from "or to any other organisation" to the end substitute "or, in such cases as it considers appropriate, to other organisations or persons, or to the general public, in the United Kingdom or elsewhere."

(3) In section 5 (warrants: general)—

(a) in subsection (2), omit ", subject to subsection (3) below,",

(b) omit subsection (3), and

(c) in subsection (3A), after "1989" insert ", or on the application of the Intelligence Service or GCHQ for the purposes of the exercise of their functions by virtue of section 1(2)(c) or 3(2)(c),".

252 National security notices

(1) The Secretary of State may give any telecommunications operator in the United Kingdom a national security notice under this section if—

(a) the Secretary of State considers that the notice is necessary in the interests of national security,

(b) the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct, and

(c) the decision to give the notice has been approved by a Judicial Commissioner.

(2) A "national security notice" is a notice requiring the operator to take such specified steps as the Secretary of State considers necessary in the interests of national security.

(3) A national security notice may, in particular, require the operator to whom it is given—

(a) to carry out any conduct, including the provision of services or facilities, for the purpose of—

(i) facilitating anything done by an intelligence service under any enactment other than this Act, or

(ii) dealing with an emergency (within the meaning of Part 1 of the Civil Contingencies Act 2004);

(b) to provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively.

(4) In a case where—

(a) a national security notice would require the taking of any steps, and

(b) in the absence of such a notice requiring the taking of those steps, the taking of those steps would be lawful only if a warrant or authorisation under a relevant enactment had been obtained,

the notice may require the taking of those steps only if such a warrant or authorisation has been obtained.

(5) But the Secretary of State may not give any telecommunications operator a national security notice the main purpose of which is to require the operator to do something for which a warrant or authorisation under a relevant enactment is required.

(6) In this section "relevant enactment" means—

(a) this Act;

(b) the Intelligence Services Act 1994;

(c) the Regulation of Investigatory Powers Act 2000;

(d) the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11).

(7) A national security notice must specify such period as appears to the Secretary of State to be reasonable as the period within which the steps specified in the notice are to be taken.

(8) Conduct required by a national security notice is to be treated as lawful for all purposes (to the extent that it would not otherwise be so treated).

(9) Sections 254 to 258 contain further provision about national security notices.

253 Technical capability notices

(1) The Secretary of State may give a relevant operator a technical capability notice under this section if—

(a) the Secretary of State considers that the notice is necessary for securing that the operator has the capability to provide any assistance which the operator may be required to provide in relation to any relevant authorisation,

(b) the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct, and

(c) the decision to give the notice has been approved by a Judicial Commissioner.

(2) A "technical capability notice" is a notice—

(a) imposing on the relevant operator any applicable obligations specified in the notice, and

(b) requiring the person to take all the steps specified in the notice for the purpose of complying with those obligations.

(3) In this section—

"applicable obligation", in relation to a relevant operator of a particular description, means an obligation specified by the Secretary of State in regulations as an obligation that may be imposed on relevant operators, or on relevant operators of that description;

"relevant authorisation" means—

(a) any warrant issued under Part 2, 5 or 6, or

(b) any authorisation or notice given under Part 3;

"relevant operator" means—

(a) a postal operator,

(b) a telecommunications operator, or

(c) a person who is proposing to become a postal operator or a telecommunications operator.

(4) Regulations under this section may specify an obligation that may be imposed on any relevant operators only if the Secretary of State considers it is reasonable to do so for the purpose of securing—

(a) that it is (and remains) practicable to impose requirements on those relevant operators to provide assistance in relation to relevant authorisations, and

(b) that it is (and remains) practicable for those relevant operators to comply with those requirements.

(5) The obligations that may be specified in regulations under this section include, among other things—

(a) obligations to provide facilities or services of a specified description;

(b) obligations relating to apparatus owned or operated by a relevant operator;

(c) obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data;

(d) obligations relating to the security of any postal or telecommunications services provided by a relevant operator;

(e) obligations relating to the handling or disclosure of any information.

(6) Before making any regulations under this section, the Secretary of State must consult the following persons—

(a) the Technical Advisory Board,

(b) persons appearing to the Secretary of State to be likely to be subject to any obligations specified in the regulations,

(c) persons representing persons falling within paragraph (b), and

(d) persons with statutory functions in relation to persons falling within that paragraph.

(7) A technical capability notice—

(a) must specify such period as appears to the Secretary of State to be reasonable as the period within which the steps specified in the notice are to be taken, and

(b) may specify different periods in relation to different steps.

(8) A technical capability notice may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United Kingdom).

(9) Sections 254 to 258 contain further provision about technical capability notices.

254 Approval of notices by Judicial Commissioners

(1) In this section "relevant notice" means—

(a) a national security notice under section 252, or

(b) a technical capability notice under section 253.

(2) In deciding whether to approve a decision to give a relevant notice, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the notice is necessary as mentioned in section 252(1)(a) or (as the case may be) section 253(1)(a), and

(b) whether the conduct that would be required by the notice is proportionate to what is sought to be achieved by that conduct.

(3) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (2) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(4) Where a Judicial Commissioner refuses to approve a decision to give a relevant notice, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(5) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to give a relevant notice, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to give the notice.

255 Further provision about notices under section 252 or 253

(1) In this section "relevant notice" means—

(a) a national security notice under section 252, or

(b) a technical capability notice under section 253.

(2) Before giving a relevant notice to a person, the Secretary of State must consult that person.

(3) Before giving a relevant notice, the Secretary of State must, among other matters, take into account—

(a) the likely benefits of the notice,

(b) the likely number of users (if known) of any postal or telecommunications service to which the notice relates,

(c) the technical feasibility of complying with the notice,

(d) the likely cost of complying with the notice, and

(e) any other effect of the notice on the person (or description of person) to whom it relates.

(4) In the case of a technical capability notice that would impose any obligations relating to the removal by a person of electronic protection applied by or on behalf of that person to any communications or data, in complying with subsection (3) the Secretary of State must in particular take into account the technical feasibility, and likely cost, of complying with those obligations.

(5) A relevant notice must be in writing.

(6) A technical capability notice may be given to a person outside the United Kingdom in any of the following ways (as well as by electronic or other means of giving a notice)—

(a) by delivering it to the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, to any place in the United Kingdom where the person carries on business or conducts activities;

(b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept documents of the same description as a notice, by delivering it to that address.

(7) The Secretary of State may by regulations make further provision about the giving of relevant notices.

(8) A person to whom a relevant notice is given, or any person employed or engaged for the purposes of that person's business, must not disclose the existence or contents of the notice to any other person without the permission of the Secretary of State.

(9) A person to whom a relevant notice is given must comply with the notice.

(10) The duty imposed by subsection (9) is enforceable—

(a) in relation to a person in the United Kingdom, and

(b) so far as relating to a technical capability notice within subsection (11), in relation to a person outside the United Kingdom,

by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

(11) A technical capability notice is within this subsection if it relates to any of the following—

(a) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2;

(b) a bulk interception warrant;

(c) an authorisation or notice given under Part 3.

(12) Subsection (9) applies to a person to whom a national security notice is given despite any other duty imposed on the person by or under Part 1, or Chapter 1 of Part 2, of the Communications Act 2003.

256 Variation and revocation of notices

(1) In this section "relevant notice" means—

(a) a national security notice under section 252, or

(b) a technical capability notice under section 253.

(2) The Secretary of State must keep each relevant notice under review.

(3) The Secretary of State may—

(a) vary a relevant notice;

(b) revoke a relevant notice (whether wholly or in part).

(4) The Secretary of State may vary a national security notice given to a person only if—

(a) the Secretary of State considers that the variation is necessary in the interests of national security,

(b) the Secretary of State considers that the conduct required by the notice as varied is proportionate to what is sought to be achieved by that conduct, and

(c) if the variation would impose further requirements on the person, the decision to vary the notice has been approved by a Judicial Commissioner (but see subsection (6)).

(5) The Secretary of State may vary a technical capability notice given to a person only if—

(a) the Secretary of State considers that the variation is necessary for securing that the person has the capability to provide any assistance which the person

may be required to provide in relation to any relevant authorisation (within the meaning of section 253),

(b) the Secretary of State considers that the conduct required by the notice as varied is proportionate to what is sought to be achieved by that conduct, and

(c) if the variation would impose further requirements on the person, the decision to vary the notice has been approved by a Judicial Commissioner (but see subsection (6)).

(6) The condition in subsection (4)(c) or (as the case may be) subsection (5)(c) does not apply in the case of a variation to which section 257(10) applies.

(7) If the Secretary of State varies or revokes a relevant notice given to any person, the Secretary of State must give that person notice of the variation or revocation.

(8) Section 254 (approval of notices by Judicial Commissioners) applies in relation to a decision to vary a relevant notice (other than a decision to which section 257(10) applies) as it applies in relation to a decision to give a relevant notice, but as if—

(a) the reference in section 254(2)(a) to the notice were to the variation, and

(b) the reference in section 254(2)(b) to the notice were to the notice as varied.

(9) Subsections (2) to (4) and (7) of section 255 apply in relation to varying or revoking a relevant notice as they apply in relation to giving a relevant notice (and in the application of section 255(3) and (4) in relation to varying a relevant notice, references to the notice are to be read as references to the notice as varied).

(10) Subsections (5) and (6) of section 255 apply to any notice of the variation or revocation of a relevant notice as they apply to a relevant notice.

(11) The fact that a relevant notice has been revoked in relation to a particular person (or description of persons) does not prevent the giving of another relevant notice of the same kind in relation to the same person (or description of persons).

(12) Any reference in this section or section 255(8) to (12) to a notice given under section 252 or 253 includes a reference to such a notice as varied under this section.

257 Review of notices by the Secretary of State

(1) A person who is given a notice under section 252 or 253 may, within such period or circumstances as may be provided for by regulations made by the Secretary of State, refer the notice back to the Secretary of State.

(2) Such a reference may be in relation to the whole of a notice or any aspect of it.

(3) There is no requirement for a person who has referred a notice under subsection (1) to comply with the notice, so far as referred, until the Secretary of State has reviewed the notice in accordance with subsection (4).

(4) The Secretary of State must review any notice so far as referred to the Secretary of State under subsection (1).

(5) Before deciding the review, the Secretary of State must consult—

(a) the Technical Advisory Board, and

(b) a Judicial Commissioner.

(6) The Board must consider the technical requirements and the financial consequences, for the person who has made the reference, of the notice so far as referred.

(7) The Commissioner must consider whether the notice so far as referred is proportionate.

(8) The Board and the Commissioner must—

(a) give the person concerned and the Secretary of State the opportunity to provide evidence, or make representations, to them before reaching their conclusions, and

(b) report their conclusions to—

(i) the person, and

(ii) the Secretary of State.

(9) The Secretary of State may, after considering the conclusions of the Board and the Commissioner—

(a) vary or revoke the notice under section 256, or

(b) give a notice under this section to the person confirming its effect.

(10) But the Secretary of State may vary the notice, or give a notice under subsection (9)(b) confirming its effect, only if the Secretary of State's decision to do so has been approved by the Investigatory Powers Commissioner.

(11) Subsections (5) to (8) of section 255 apply in relation to a notice under subsection (9)(b) above as they apply in relation to a notice under section 252 or 253.

(12) Any reference in this section or section 258 to a notice under section 252 or 253 includes such a notice as varied under section 256, but only so far as the variation is concerned.

But it does not include a notice varied as mentioned in subsection (9)(a) above.

258 Approval of notices following review under section 257

(1) In this section "relevant notice" means—

(a) a national security notice under section 252, or

(b) a technical capability notice under section 253.

(2) In deciding whether to approve a decision to vary a relevant notice as mentioned in section 257(9)(a), or to give a notice under section 257(9)(b) confirming the effect of a relevant notice, the Investigatory Powers Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the relevant notice as varied or confirmed is necessary as mentioned in section 252(1)(a) or (as the case may be) section 253(1)(a), and

(b) whether the conduct required by the relevant notice, as varied or confirmed, is proportionate to what is sought to be achieved by that conduct.

(3) In doing so, the Investigatory Powers Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (2) with a sufficient degree of care as to ensure that the Investigatory Powers Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(4) Where the Investigatory Powers Commissioner refuses to approve a decision to vary a relevant notice as mentioned in section 257(9)(a), or to give a notice under

section 257(9)(b) confirming the effect of a relevant notice, the Investigatory Powers Commissioner must give the Secretary of State written reasons for the refusal.

Wireless telegraphy

259 Amendments of the Wireless Telegraphy Act 2006

(1) The Wireless Telegraphy Act 2006 is amended as follows.

(2) Section 48 (interception and disclosure of messages) is amended as follows.

(3) In subsection (1), for "otherwise than under the authority of a designated person" substitute "without lawful authority".

(4) After subsection (3) insert—

"(3A) A person does not commit an offence under this section consisting in any conduct if the conduct—

(a) constitutes an offence under section 3(1) of the Investigatory Powers Act 2016 (offence of unlawful interception), or

(b) would do so in the absence of any lawful authority (within the meaning of section 6 of that Act)."

(5) Omit subsection (5).

(6) Omit section 49 (interception authorities).

(7) In consequence of the repeal made by subsection (6)—

(a) in sections 50(5) and 119(2)(a), for "49" substitute "48";

(b) in section 121(2), omit paragraph (b).

CHAPTER 2

GENERAL

Review of operation of Act

260 Review of operation of Act

(1) The Secretary of State must, within the period of 6 months beginning with the end of the initial period, prepare a report on the operation of this Act.

(2) In subsection (1) "the initial period" is the period of 5 years and 6 months beginning with the day on which this Act is passed.

(3) In preparing the report under subsection (1), the Secretary of State must, in particular, take account of any report on the operation of this Act made by a Select Committee of either House of Parliament (whether acting alone or jointly).

(4) The Secretary of State must—

(a) publish the report prepared under subsection (1), and

(b) lay a copy of it before Parliament.

Interpretation

261 Telecommunications definitions

(1) The definitions in this section have effect for the purposes of this Act.

Communication

(2) "Communication", in relation to a telecommunications operator, telecommunications service or telecommunication system, includes—

(a) anything comprising speech, music, sounds, visual images or data of any description, and

(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.

Entity data

(3) "Entity data" means any data which—

(a) is about—

(i) an entity,

(ii) an association between a telecommunications service and an entity, or

(iii) an association between any part of a telecommunication system and an entity,

(b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and

(c) is not events data.

Events data

(4) "Events data" means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.

Communications data

(5) "Communications data", in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data—

(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—

(i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,

(ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or

(iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,

(b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or

(c) which—

(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,

(ii) is about the architecture of a telecommunication system, and

(iii) is not about a specific person,

but does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication.

Content of a communication

(6) "Content", in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—

(a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and

(b) anything which is systems data is not content.

Other definitions

(7) "Entity" means a person or thing.

(8) "Public telecommunications service" means any telecommunications service which is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom.

(9) "Public telecommunication system" means a telecommunication system located in the United Kingdom—

(a) by means of which any public telecommunications service is provided, or

(b) which consists of parts of any other telecommunication system by means of which any such service is provided.

(10) "Telecommunications operator" means a person who—

(a) offers or provides a telecommunications service to persons in the United Kingdom, or

(b) controls or provides a telecommunication system which is (wholly or partly) —

(i) in the United Kingdom, or

(ii) controlled from the United Kingdom.

(11) "Telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service).

(12) For the purposes of subsection (11), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system.

(13) "Telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the

purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy.

(14) "Private telecommunication system" means any telecommunication system which—

(a) is not a public telecommunication system,

(b) is attached, directly or indirectly, to a public telecommunication system (whether or not for the purposes of the communication in question), and

(c) includes apparatus which is both located in the United Kingdom and used (with or without other apparatus) for making the attachment to that public telecommunication system.

262 Postal definitions

(1) The definitions in this section have effect for the purposes of this Act.

Communication

(2) "Communication", in relation to a postal operator or postal service (but not in the definition of "postal service" in this section), includes anything transmitted by a postal service.

Communications data

(3) "Communications data", in relation to a postal operator or postal service, means—

(a) postal data comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a postal service by means of which it is being or may be transmitted,

(b) information about the use made by any person of a postal service (but excluding any content of a communication (apart from information within paragraph (a)), or

(c) information not within paragraph (a) or (b) that is (or is to be or is capable of being) held or obtained by or on behalf of a person providing a postal service, is about those to whom the service is provided by that person and relates to the service so provided.

Postal data

(4) "Postal data" means data which—

(a) identifies, or purports to identify, any person, apparatus or location to or from which a communication is or may be transmitted,

(b) identifies or selects, or purports to identify or select, apparatus through which, or by means of which, a communication is or may be transmitted,

(c) identifies, or purports to identify, the time at which an event relating to a communication occurs, or

(d) identifies the data or other data as data comprised in, included as part of, attached to or logically associated with a particular communication.

For the purposes of this definition "data", in relation to a postal item, includes anything written on the outside of the item.

Other definitions

(5) "Postal item" means—

(a) any letter, postcard or other such thing in writing as may be used by the sender for imparting information to the recipient, or

(b) any packet or parcel.

(6) "Postal operator" means a person providing a postal service to persons in the United Kingdom.

(7) "Postal service" means a service that—

(a) consists in the following, or in any one or more of them, namely, the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items, and

(b) has as its main purpose, or one of its main purposes, to make available, or to facilitate, a means of transmission from place to place of postal items containing communications.

(8) "Public postal service" means a postal service that is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom.

263 General definitions

(1) In this Act—

"apparatus" includes any equipment, machinery or device (whether physical or logical) and any wire or cable,

"civil proceedings" means any proceedings in or before any court or tribunal that are not criminal proceedings,

"crime" means conduct which—

(a) constitutes one or more criminal offences, or

(b) is, or corresponds to, any conduct which, if it all took place in any one part of the United Kingdom, would constitute one or more criminal offences,

"criminal proceedings" includes proceedings before a court in respect of a service offence within the meaning of the Armed Forces Act 2006 (and references to criminal prosecutions are to be read accordingly),

"data" includes data which is not electronic data and any information (whether or not electronic),

"destroy", in relation to electronic data, means delete the data in such a way as to make access to the data impossible (and related expressions are to be read accordingly),

"enactment" means an enactment whenever passed or made; and includes—

(a) an enactment contained in subordinate legislation within the meaning of the Interpretation Act 1978,

(b) an enactment contained in, or in an instrument made under, an Act of the Scottish Parliament,

(c) an enactment contained in, or in an instrument made under, a Measure or Act of the National Assembly for Wales, and

(d) an enactment contained in, or in an instrument made under, Northern Ireland legislation,

"enhanced affirmative procedure" is to be read in accordance with section 268,

"functions" includes powers and duties,

"GCHQ" has the same meaning as in the Intelligence Services Act 1994,

"head", in relation to an intelligence service, means—

(a) in relation to the Security Service, the Director-General,

(b) in relation to the Secret Intelligence Service, the Chief, and

(c) in relation to GCHQ, the Director,

"Her Majesty's forces" has the same meaning as in the Armed Forces Act 2006,

"identifying data" has the meaning given by subsection (2),

"intelligence service" means the Security Service, the Secret Intelligence Service or GCHQ,

"the Investigatory Powers Commissioner" means the person appointed under section 227(1)(a) (and the expression is also to be read in accordance with section 227(13)(b)),

"the Investigatory Powers Tribunal" means the tribunal established under section 65 of the Regulation of Investigatory Powers Act 2000,

"items subject to legal privilege"—

(a) in relation to England and Wales, has the same meaning as in the Police and Criminal Evidence Act 1984 (see section 10 of that Act),

(b) in relation to Scotland, means—

(i) communications between a professional legal adviser and the adviser's client, or

(ii) communications made in connection with, or in contemplation of, legal proceedings and for the purposes of those proceedings,

which would, by virtue of any rule of law relating to the confidentiality of communications, be protected in legal proceedings from disclosure, and

(c) in relation to Northern Ireland, has the same meaning as in the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989/1341 (N.I. 12)) (see Article 12 of that Order),

"Judicial Commissioner" means a person appointed under section 227(1)(a) or (b) (and the expression is therefore to be read in accordance with section 227(13)(a)),

"legal proceedings" means—

(a) civil or criminal proceedings in or before a court or tribunal, or

(b) proceedings before an officer in respect of a service offence within the meaning of the Armed Forces Act 2006,

"modify" includes amend, repeal or revoke (and related expressions are to be read accordingly),

"person holding office under the Crown" includes any servant of the Crown and any member of Her Majesty's forces,

"premises" includes any land, movable structure, vehicle, vessel, aircraft or hovercraft (and "set of premises" is to be read accordingly),

"primary legislation" means—

(a) an Act of Parliament,

(b) an Act of the Scottish Parliament,

(c) a Measure or Act of the National Assembly for Wales, or

(d) Northern Ireland legislation,

"public authority" means a public authority within the meaning of section 6 of the Human Rights Act 1998, other than a court or tribunal,

"serious crime" means crime where—

(a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or

(b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose,

"source of journalistic information" means an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used,

"specified", in relation to an authorisation, warrant, notice or regulations, means specified or described in the authorisation, warrant, notice or (as the case may be) regulations (and "specify" is to be read accordingly),

"statutory", in relation to any function, means conferred by virtue of this Act or any other enactment,

"subordinate legislation" means—

(a) subordinate legislation within the meaning of the Interpretation Act 1978, or

(b) an instrument made under an Act of the Scottish Parliament, Northern Ireland legislation or a Measure or Act of the National Assembly for Wales,

"systems data" has the meaning given by subsection (4),

"the Technical Advisory Board" means the Board provided for by section 245,

"the Technology Advisory Panel" means the panel established in accordance with section 246(1),

"working day" means a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom.

(2) In this Act "identifying data" means—

(a) data which may be used to identify, or assist in identifying, any person, apparatus, system or service,

(b) data which may be used to identify, or assist in identifying, any event, or

(c) data which may be used to identify, or assist in identifying, the location of any person, event or thing.

(3) For the purposes of subsection (2), the reference to data which may be used to identify, or assist in identifying, any event includes—

(a) data relating to the fact of the event;

(b) data relating to the type, method or pattern of event;

(c) data relating to the time or duration of the event.

(4) In this Act "systems data" means any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following—

(a) a postal service;

(b) a telecommunication system (including any apparatus forming part of the system);

(c) any telecommunications service provided by means of a telecommunication system;

(d) a relevant system (including any apparatus forming part of the system);

(e) any service provided by means of a relevant system.

(5) For the purposes of subsection (4), a system is a "relevant system" if any communications or other information are held on or by means of the system.

(6) For the purposes of this Act detecting crime or serious crime is to be taken to include—

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime or (as the case may be) serious crime was committed, and

(b) the apprehension of the person by whom any crime or (as the case may be) serious crime was committed.

(7) References in this Act to the examination of material obtained under a warrant are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.

264 General definitions: "journalistic material" etc.

(1) The definitions in this section have effect for the purposes of this Act.

Journalistic material

(2) "Journalistic material" means material created or acquired for the purposes of journalism.

(3) For the purposes of this section, where—

(a) a person ("R") receives material from another person ("S"), and

(b) S intends R to use the material for the purposes of journalism,

R is to be taken to have acquired it for those purposes.

Accordingly, a communication sent by S to R containing such material is to be regarded as a communication containing journalistic material.

(4) For the purposes of determining whether a communication contains material acquired for the purposes of journalism, it does not matter whether the material has been acquired for those purposes by the sender or recipient of the communication or by some other person.

(5) For the purposes of this section—

(a) material is not to be regarded as created or acquired for the purposes of journalism if it is created or acquired with the intention of furthering a criminal purpose, and

(b) material which a person intends to be used to further such a purpose is not to be regarded as intended to be used for the purposes of journalism.

Confidential journalistic material

(6) "Confidential journalistic material" means—

(a) in the case of material contained in a communication, journalistic material which the sender of the communication—

(i) holds in confidence, or

(ii) intends the recipient, or intended recipient, of the communication to hold in confidence;

(b) in any other case, journalistic material which a person holds in confidence.

(7) A person holds material in confidence for the purposes of this section if—

(a) the person holds it subject to an express or implied undertaking to hold it in confidence, or

(b) the person holds it subject to a restriction on disclosure or an obligation of secrecy contained in an enactment.

265 Index of defined expressions

In this Act, the expressions listed in the left-hand column have the meaning given by, or are to be interpreted in accordance with, the provisions listed in the right-hand column.

Expression	*Provision*
Apparatus	Section 263(1)
Bulk equipment interference warrant	Section 176(1)
Bulk interception warrant	Section 136(1)
Civil proceedings	Section 263(1)
Communication	Sections 261(2) and 262(2)
Communications data	Sections 261(5) and 262(3)
Confidential journalistic material	Section 264(6) and (7)
Content of a communication (in relation to a telecommunications operator, telecommunications service or telecommunication system)	Section 261(6)
Crime	Section 263(1)
Criminal proceedings	Section 263(1)
Criminal prosecution	Section 263(1)
Data	Section 263(1)
Destroy (in relation to electronic data) and related expressions	Section 263(1)
Detecting crime or serious crime	Section 263(6)
Enactment	Section 263(1)
Enhanced affirmative procedure	Section 263(1)

Expression	*Provision*
Entity	Section 261(7)
Entity data	Section 261(3)
Events data	Section 261(4)
Examination (in relation to material obtained under a warrant)	Section 263(7)
Functions	Section 263(1)
GCHQ	Section 263(1)
Head (in relation to an intelligence service)	Section 263(1)
Her Majesty's forces	Section 263(1)
Identifying data	Section 263(2) and (3)
Intelligence service	Section 263(1)
Interception of communication (postal service)	Sections 4(7) and 5
Interception of communication (telecommunication system)	Sections 4(1) to (6) and 5(1)
Interception of communication in the United Kingdom	Section 4(8)
Internet connection record	Section 62(7)
Investigatory Powers Commissioner	Section 263(1)
Investigatory Powers Tribunal	Section 263(1)
Items subject to legal privilege	Section 263(1)
Journalistic material	Section 264(2) to (5)
Judicial Commissioner	Section 263(1)
Judicial Commissioners	Section 227(7)
Lawful authority (in relation to interception of communication)	Section 6
Legal proceedings	Section 263(1)
Modify (and related expressions)	Section 263(1)
Person holding office under the Crown	Section 263(1)
Postal data	Section 262(4)
Postal item	Section 262(5)
Postal item in course of transmission by postal service	Section 4(7)
Postal operator	Section 262(6)
Postal service	Section 262(7)
Premises	Section 263(1)
Primary legislation	Section 263(1)

Expression	*Provision*
Private telecommunication system	Section 261(14)
Public authority	Section 263(1)
Public postal service	Section 262(8)
Public telecommunications service	Section 261(8)
Public telecommunication system	Section 261(9)
Serious crime	Section 263(1) (and paragraph 6 of Schedule 9)
Source of journalistic information	Section 263(1)
Specified and specify (in relation to an authorisation, warrant, notice or regulations)	Section 263(1)
Statutory (in relation to any function)	Section 263(1)
Subordinate legislation	Section 263(1)
Systems data	Section 263(4) and (5)
Technical Advisory Board	Section 263(1)
Technology Advisory Panel	Section 263(1)
Telecommunications operator	Section 261(10)
Telecommunications service	Section 261(11) and (12)
Telecommunication system	Section 261(13)
Working day	Section 263(1)

Supplementary provision

266 Offences by bodies corporate etc.

(1) This section applies if an offence under this Act is committed by a body corporate or a Scottish partnership.

(2) If the offence is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of—

(a) a senior officer of the body corporate or Scottish partnership, or

(b) a person purporting to act in such a capacity,

the senior officer or person (as well as the body corporate or partnership) is guilty of the offence and liable to be proceeded against and punished accordingly.

(3) In this section—

"director", in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate,

"senior officer" means—

(a) in relation to a body corporate, a director, manager, secretary or other similar officer of the body corporate, and

(b) in relation to a Scottish partnership, a partner in the partnership.

267 Regulations

(1) Any power of the Secretary of State or the Treasury to make regulations under this Act—

(a) is exercisable by statutory instrument,

(b) may be exercised so as to make different provision for different purposes or different areas, and

(c) includes power to make supplementary, incidental, consequential, transitional, transitory or saving provision.

(2) See sections 72(3) and 73(6) for the procedure for a statutory instrument containing regulations under section 71 to which section 72 applies or (as the case may be) regulations under section 73(4) to which section 73(5) applies (enhanced affirmative procedure).

(3) A statutory instrument containing regulations under—

(a) section 12(4) or 271(2) which amend or repeal any provision of primary legislation,

(b) section 46(2),

(c) section 52(5),

(d) section 83,

(e) section 90(1),

(f) section 239,

(g) section 240(3),

(h) section 245,

(i) section 253,

(j) section 257(1), or

(k) paragraph 33 of Schedule 8,

may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.

(4) A statutory instrument containing—

(a) regulations under section 12(4) or 271(2) to which subsection (3) does not apply,

(b) regulations under section 65(5), or

(c) regulations under paragraph 2(1)(b) of Schedule 5,

is (if a draft of the instrument has not been laid before, and approved by a resolution of, each House of Parliament) subject to annulment in pursuance of a resolution of either House of Parliament.

(5) A statutory instrument containing—

(a) regulations under section 10(3),

(b) regulations under section 52(3),

(c) regulations under section 58(8)(a),

(d) regulations under section 71 to which section 72 does not apply,

(e) regulations under section 73(4) to which section 73(5) does not apply,

(f) regulations under section 133(6)(a), or

(g) regulations under section 255(7),

is subject to annulment in pursuance of a resolution of either House of Parliament.

(6) A statutory instrument containing regulations under paragraph 4 of Schedule 5 is subject to annulment in pursuance of a resolution of the House of Commons.

(7) See paragraphs 4(4) and 5(5) of Schedule 7 for the procedure for a statutory instrument containing regulations about the coming into force of a code of practice under that Schedule or of any revisions to such a code of practice (affirmative procedure or, in the case of the coming into force of revisions, a choice between that procedure and laying before Parliament after being made).

(8) A statutory instrument containing regulations which are subject to a particular parliamentary procedure under this Act may also include regulations which are subject to a different or no parliamentary procedure under this Act (but this subsection does not apply to regulations mentioned in subsection (2), (4), (6) or (7)).

(9) A statutory instrument which, by virtue of subsection (8), contains regulations which are subject to different parliamentary procedures, or one or more parliamentary procedure and no parliamentary procedure, is subject to whichever procedure is the higher procedure; and the order is as follows (the highest first)—

(a) the procedure set out in subsection (3) (the affirmative procedure),

(b) the procedure set out in subsection (5) above (the negative procedure),

(c) no procedure.

(10) Provision is not prevented from being included in regulations made under this Act merely because the provision could have been included in other regulations made under this Act which would have been subject to a different or no parliamentary procedure.

268 Enhanced affirmative procedure

(1) For the purposes of regulations under section 71 to which section 72 applies and regulations under section 73(4) to which section 73(5) applies, the enhanced affirmative procedure is as follows.

(2) Subsection (3) applies if—

(a) the Secretary of State has consulted under section 72(2) or (as the case may be) 73(5) in relation to making such regulations,

(b) a period of at least 12 weeks, beginning with the day on which any such consultation first began, has elapsed, and

(c) the Secretary of State considers it appropriate to proceed with making such regulations.

(3) The Secretary of State must lay before Parliament—

(a) draft regulations, and

(b) a document which explains the regulations.

(4) The Secretary of State may make regulations in the terms of the draft regulations laid under subsection (3) if, after the end of the 40-day period, the draft regulations are approved by a resolution of each House of Parliament.

(5) But subsections (6) to (9) apply instead of subsection (4) if—

(a) either House of Parliament so resolves within the 30-day period, or

(b) a committee of either House charged with reporting on the draft regulations so recommends within the 30-day period and the House to which the

recommendation is made does not by resolution reject the recommendation within that period.

(6) The Secretary of State must have regard to—

(a) any representations,

(b) any resolution of either House of Parliament, and

(c) any recommendations of a committee of either House of Parliament charged with reporting on the draft regulations,

made during the 60-day period with regard to the draft regulations.

(7) If after the end of the 60-day period the draft regulations are approved by a resolution of each House of Parliament, the Secretary of State may make regulations in the terms of the draft regulations.

(8) If after the end of the 60-day period the Secretary of State wishes to proceed with the draft regulations but with material changes, the Secretary of State may lay before Parliament—

(a) revised draft regulations, and

(b) a statement giving a summary of the changes proposed.

(9) If the revised draft regulations are approved by a resolution of each House of Parliament, the Secretary of State may make regulations in the terms of the revised draft regulations.

(10) For the purposes of this section regulations are made in the terms of draft regulations or revised draft regulations if they contain no material changes to the provisions of the draft, or revised draft, regulations.

(11) References in this section to the "30-day", "40-day" and "60-day" periods in relation to any draft regulations are to the periods of 30, 40 and 60 days beginning with the day on which the draft regulations were laid before Parliament; and, for this purpose, no account is to be taken of any time during which Parliament is dissolved or prorogued or during which either House is adjourned for more than four days.

269 Financial provisions

There is to be paid out of money provided by Parliament—

(a) any expenditure incurred by a Minister of the Crown or government department by virtue of this Act, and

(b) any increase attributable to this Act in the sums payable by virtue of any other Act out of money so provided.

270 Transitional, transitory or saving provision

(1) Schedule 9 (which contains transitional, transitory and saving provision including a general saving for lawful conduct) has effect.

(2) The Secretary of State may by regulations make such transitional, transitory or saving provision as the Secretary of State considers appropriate in connection with the coming into force of any provision of this Act.

271 Minor and consequential provision

(1) Schedule 10 (which contains minor and consequential provision) has effect.

(2) The Secretary of State may by regulations make such provision as the Secretary of State considers appropriate in consequence of this Act.

(3) The power to make regulations under subsection (2) may, in particular, be exercised by modifying any provision made by or under an enactment.

(4) In subsection (3) "enactment" does not include any primary legislation passed or made after the end of the Session in which this Act is passed.

Final provision

272 Commencement, extent and short title

(1) Subject to subsections (2) and (3), this Act comes into force on such day as the Secretary of State may by regulations appoint; and different days may be appointed for different purposes.

(2) Sections 260 to 269, 270(2), 271(2) to (4) and this section come into force on the day on which this Act is passed.

(3) Sections 227 and 228 come into force at the end of the period of two months beginning with the day on which this Act is passed.

(4) Subject to subsections (5) to (7), this Act extends to England and Wales, Scotland and Northern Ireland.

(5) An amendment, repeal or revocation made by this Act of an enactment has the same extent within the United Kingdom as the enactment amended, repealed or revoked.

(6) Her Majesty may by Order in Council provide for any of the provisions of this Act to extend, with or without modifications, to the Isle of Man or any of the British overseas territories.

(7) Any power under an Act to extend any provision of that Act by Order in Council to any of the Channel Islands may be exercised so as to extend there (with or without modifications) any amendment or repeal of that provision which is made by or under this Act.

(8) This Act may be cited as the Investigatory Powers Act 2016.