

# Investigatory Powers Bill

---

---

## EXPLANATORY NOTES

Explanatory notes to the Bill, prepared by the Home Office, are published separately as Bill 143 – EN.

## EUROPEAN CONVENTION ON HUMAN RIGHTS

Secretary Theresa May has made the following statement under section 19(1)(a) of the Human Rights Act 1998:

In my view the provisions of the Investigatory Powers Bill are compatible with the Convention rights.

# Investigatory Powers Bill

---

---

## CONTENTS

### PART 1

#### GENERAL PRIVACY PROTECTIONS

##### *Overview of Act*

1 Overview of Act

##### *Prohibitions against unlawful interception*

- 2 Offence of unlawful interception
- 3 Definition of “interception” etc.
- 4 Conduct that is not interception
- 5 Definition of “lawful authority”
- 6 Monetary penalties for certain unlawful interceptions
- 7 Restriction on requesting interception by overseas authorities
- 8 Restriction on requesting assistance under mutual assistance agreements etc.

##### *Prohibition against unlawful obtaining of communications data*

9 Offence of unlawfully obtaining communications data

##### *Abolition of powers to obtain communications data*

10 Abolition or restriction of certain powers to obtain communications data

##### *Restrictions on interference with equipment*

- 11 Mandatory use of equipment interference warrants
- 12 Restriction on use of section 93 of the Police Act 1997

**PART 2**

## LAWFUL INTERCEPTION OF COMMUNICATIONS

**CHAPTER 1**

## INTERCEPTION AND EXAMINATION WITH A WARRANT

*Warrants under this Chapter*

- 13 Warrants that may be issued under this Chapter
- 14 Obtaining secondary data
- 15 Subject-matter of warrants

*Power to issue warrants*

- 16 Persons who may apply for issue of a warrant
- 17 Power of Secretary of State to issue warrants
- 18 Grounds on which warrants may be issued by Secretary of State
- 19 Power of Scottish Ministers to issue warrants
- 20 “Relevant Scottish applications”

*Approval of warrants by Judicial Commissioners*

- 21 Approval of warrants by Judicial Commissioners
- 22 Approval of warrants issued in urgent cases
- 23 Failure to approve warrant issued in urgent case

*Additional safeguards*

- 24 Members of Parliament etc.
- 25 Items subject to legal privilege

*Further provision about warrants*

- 26 Decisions to issue warrants to be taken personally by Ministers
- 27 Requirements that must be met by warrants
- 28 Duration of warrants
- 29 Renewal of warrants
- 30 Modification of warrants
- 31 Approval of major modifications made in urgent cases
- 32 Cancellation of warrants
- 33 Special rules for certain mutual assistance warrants

*Implementation of warrants*

- 34 Implementation of warrants
- 35 Service of warrants outside the United Kingdom
- 36 Duty of operators to assist with implementation

**CHAPTER 2**

## OTHER FORMS OF LAWFUL INTERCEPTION

*Interception with consent*

- 37 Interception with the consent of the sender or recipient

*Interception for administrative or enforcement purposes*

- 38 Interception by providers of postal or telecommunications services  
39 Interception by businesses etc. for monitoring and record-keeping purposes  
40 Postal services: interception for enforcement purposes  
41 Interception by OFCOM in connection with wireless telegraphy

*Interception taking place in certain institutions*

- 42 Interception in prisons  
43 Interception in psychiatric hospitals etc.  
44 Interception in immigration detention facilities

*Interception in accordance with overseas requests*

- 45 Interception in accordance with overseas requests

**CHAPTER 3**

## OTHER PROVISIONS ABOUT INTERCEPTION

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

- 46 Safeguards relating to retention and disclosure of material  
47 Safeguards relating to disclosure of material overseas  
48 Exclusion of matters from legal proceedings  
49 Duty not to make unauthorised disclosures  
50 Section 49: meaning of “excepted disclosure”  
51 Offence of making unauthorised disclosures

*Interpretation*

- 52 Part 2: interpretation

**PART 3**

## AUTHORISATIONS FOR OBTAINING COMMUNICATIONS DATA

*Targeted authorisations for obtaining data*

- 53 Power to grant authorisations  
54 Additional restrictions on grant of authorisations  
55 Procedure for authorisations and authorised notices  
56 Duration and cancellation of authorisations and notices  
57 Duties of telecommunications operators in relation to authorisations

*Filtering arrangements for obtaining data*

- 58 Filtering arrangements for obtaining data
- 59 Use of filtering arrangements in pursuance of an authorisation
- 60 Duties in connection with operation of filtering arrangements

*Relevant public authorities other than local authorities*

- 61 Relevant public authorities and designated senior officers
- 62 Power to modify section 61 and Schedule 4
- 63 Certain regulations under section 62: supplementary

*Local authorities*

- 64 Local authorities as relevant public authorities
- 65 Requirement to be party to collaboration agreement
- 66 Judicial approval for local authority authorisations

*Additional protections*

- 67 Use of a single point of contact
- 68 Commissioner approval for authorisations to identify or confirm journalistic sources

*Collaboration agreements*

- 69 Collaboration agreements
- 70 Collaboration agreements: supplementary
- 71 Police collaboration agreements

*Further and supplementary provision*

- 72 Lawfulness of conduct authorised by this Part
- 73 Offence of making unauthorised disclosure
- 74 Certain transfer and agency arrangements with public authorities
- 75 Application of Part 3 to postal operators and postal services
- 76 Extra-territorial application of Part 3
- 77 Part 3: interpretation

**PART 4**

## RETENTION OF COMMUNICATIONS DATA

*General*

- 78 Powers to require retention of certain data

*Safeguards*

- 79 Matters to be taken into account before giving retention notices
- 80 Review by the Secretary of State
- 81 Data integrity and security
- 82 Disclosure of retained data

*Variation or revocation of notices*

- 83 Variation or revocation of notices

*Enforcement*

- 84 Enforcement of notices and certain other requirements and restrictions

*Further and supplementary provision*

- 85 Application of Part 4 to postal operators and postal services  
86 Extra-territorial application of Part 4  
87 Part 4: interpretation

**PART 5**

## EQUIPMENT INTERFERENCE

*Warrants under this Part*

- 88 Warrants under this Part: general  
89 Meaning of “equipment data”  
90 Subject-matter of warrants

*Power to issue warrants*

- 91 Power to issue warrants to intelligence services: the Secretary of State  
92 Power to issue warrants to intelligence services: the Scottish Ministers  
93 Power to issue warrants to the Chief of Defence Intelligence  
94 Members of Parliament etc.  
95 Decision to issue warrants under sections 91 to 93 to be taken personally by Ministers  
96 Power to issue warrants to law enforcement officers

*Approval of warrants by Judicial Commissioners*

- 97 Approval of warrants by Judicial Commissioners  
98 Approval of warrants issued in urgent cases  
99 Failure to approve warrant issued in urgent case

*Additional safeguards*

- 100 Items subject to legal privilege

*Further provision about warrants*

- 101 Requirements which must be met by warrants  
102 Duration of warrants  
103 Renewal of warrants  
104 Modification of warrants issued by the Secretary of State or Scottish Ministers  
105 Approval of modifications under section 104 made in urgent cases  
106 Modification of warrants issued by law enforcement chiefs  
107 Approval of modifications under section 106 in urgent cases  
108 Cancellation of warrants

*Implementation of warrants*

- 109 Implementation of warrants
- 110 Service of warrants outside the United Kingdom
- 111 Duty of telecommunications operators to assist with implementation

*Supplementary provision*

- 112 Safeguards relating to retention and disclosure of material
- 113 Safeguards relating to disclosure of material or data overseas
- 114 Duty not to make unauthorised disclosures
- 115 Section 114: meaning of “excepted” disclosure
- 116 Offence of making unauthorised disclosure
- 117 Restriction on issue of warrants to certain law enforcement officers
- 118 Part 5: interpretation

**PART 6****BULK WARRANTS****CHAPTER 1****BULK INTERCEPTION WARRANTS***Bulk interception warrants*

- 119 Bulk interception warrants
- 120 Obtaining secondary data
- 121 Power to issue bulk interception warrants
- 122 Additional requirements in respect of warrants affecting overseas operators
- 123 Approval of warrants by Judicial Commissioners
- 124 Decisions to issue warrants to be taken personally by Secretary of State
- 125 Requirements that must be met by warrants

*Duration, modification and cancellation of warrants*

- 126 Duration of warrants
- 127 Renewal of warrants
- 128 Modification of warrants
- 129 Approval of major modifications made in urgent cases
- 130 Cancellation of warrants

*Implementation of warrants*

- 131 Implementation of warrants

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

- 132 Safeguards relating to retention and disclosure of material
- 133 Safeguards relating to disclosure of material overseas
- 134 Safeguards relating to examination of material
- 135 Additional safeguards for items subject to legal privilege
- 136 Application of other restrictions in relation to warrants

*Interpretation*

137 Chapter 1: interpretation

**CHAPTER 2****BULK ACQUISITION WARRANTS***Bulk acquisition warrants*

138 Power to issue bulk acquisition warrants  
139 Approval of warrants by Judicial Commissioners  
140 Decisions to issue warrants to be taken personally by Secretary of State  
141 Requirements that must be met by warrants

*Duration, modification and cancellation of warrants*

142 Duration of warrants  
143 Renewal of warrants  
144 Modification of warrants  
145 Approval of major modifications made in urgent cases  
146 Cancellation of warrants

*Implementation of warrants*

147 Implementation of warrants  
148 Service of warrants outside the United Kingdom  
149 Duty of operators to assist with implementation

*Restrictions on use or disclosure of data obtained under warrants etc.*

150 Safeguards relating to the retention and disclosure of data  
151 Safeguards relating to examination of data

*Supplementary provision*

152 Offence of making unauthorised disclosure  
153 Chapter 2: interpretation

**CHAPTER 3****BULK EQUIPMENT INTERFERENCE WARRANTS***Bulk equipment interference warrants*

154 Bulk equipment interference warrants: general  
155 Meaning of “equipment data”  
156 Power to issue bulk equipment interference warrants  
157 Approval of warrants by Judicial Commissioners  
158 Approval of warrants issued in urgent cases  
159 Failure to approve warrant issued in urgent case  
160 Decisions to issue warrants to be taken personally by Secretary of State  
161 Requirements that must be met by warrants



*Duration, modification and cancellation of warrants*

- 162 Duration of warrants
- 163 Renewal of warrants
- 164 Modification of warrants
- 165 Approval of major modifications made in urgent cases
- 166 Cancellation of warrants

*Implementation of warrants*

- 167 Implementation of warrants

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

- 168 Safeguards relating to retention and disclosure of material
- 169 Safeguards relating to disclosure of material or data overseas
- 170 Safeguards relating to examination of material etc.
- 171 Additional safeguards for items subject to legal privilege
- 172 Application of other restrictions in relation to warrants

*Interpretation*

- 173 Chapter 3: interpretation

**PART 7****BULK PERSONAL DATASET WARRANTS***Bulk personal datasets: interpretation*

- 174 Bulk personal datasets: interpretation

*Requirement for warrant*

- 175 Requirement for authorisation by warrant: general
- 176 Exceptions to section 175(1) and (2)

*Issue of warrants*

- 177 Class BPD warrants
- 178 Specific BPD warrants
- 179 Approval of warrants by Judicial Commissioners
- 180 Approval of specific BPD warrants issued in urgent cases
- 181 Failure to approve specific BPD warrant issued in urgent case
- 182 Decisions to issue warrants to be taken personally by Secretary of State
- 183 Requirements that must be met by warrants

*Duration, modification and cancellation*

- 184 Duration of warrants
- 185 Renewal of warrants
- 186 Modification of warrants
- 187 Approval of major modifications made in urgent cases
- 188 Cancellation of warrants
- 189 Non-renewal or cancellation of BPD warrants

*Further and supplementary provision*

- 190 Initial examinations: time limits
- 191 Safeguards relating to examination of bulk personal datasets
- 192 Application of Part to bulk personal datasets obtained under this Act
- 193 Interpretation of Part

**PART 8**

## OVERSIGHT ARRANGEMENTS

**CHAPTER 1**

## INVESTIGATORY POWERS COMMISSIONER AND OTHER JUDICIAL COMMISSIONERS

*The Commissioners*

- 194 Investigatory Powers Commissioner and other Judicial Commissioners
- 195 Terms and conditions of appointment

*Main functions of Commissioners*

- 196 Main oversight functions
- 197 Additional directed oversight functions
- 198 Error reporting
- 199 Additional functions under this Part
- 200 Functions under other Parts and other enactments

*Reports and investigation and information powers*

- 201 Annual and other reports
- 202 Investigation and information powers
- 203 Information gateway

*Supplementary provision*

- 204 Funding, staff and facilities
- 205 Power to modify functions
- 206 Abolition of existing oversight bodies

**CHAPTER 2**

## OTHER ARRANGEMENTS

*Codes of practice*

- 207 Codes of practice

*Investigatory Powers Tribunal*

- 208 Right of appeal from Tribunal
- 209 Functions of Tribunal in relation to this Act

*Information Commissioner*

- 210 Oversight by Information Commissioner in relation to Part 4

*Technical Advisory Board*

- 211 Technical Advisory Board

**PART 9**

## MISCELLANEOUS AND GENERAL PROVISIONS

**CHAPTER 1**

## MISCELLANEOUS

*Combined warrants and authorisations*

- 212 Combination of warrants and authorisations

*Compliance with Act*

- 213 Payments towards certain compliance costs  
214 Power to develop compliance systems etc.

*Additional powers*

- 215 Amendments of the Intelligence Services Act 1994  
216 National security notices  
217 Maintenance of technical capability  
218 Further provision about notices under section 216 or 217  
219 Variation and revocation of notices  
220 Review by the Secretary of State

*Wireless telegraphy*

- 221 Amendments of the Wireless Telegraphy Act 2006

**CHAPTER 2**

## GENERAL

*Review of operation of Act*

- 222 Review of operation of Act

*Interpretation*

- 223 Telecommunications definitions  
224 Postal definitions  
225 General definitions  
226 Index of defined expressions

*Supplementary provision*

- 227 Offences by bodies corporate etc.
- 228 Regulations
- 229 Enhanced affirmative procedure
- 230 Financial provisions
- 231 Transitional, transitory or saving provision
- 232 Minor and consequential provision

*Final provision*

- 233 Commencement, extent and short title

- 
- Schedule 1 – Monetary penalty notices
    - Part 1 – Monetary penalty notices
    - Part 2 – Information provisions
  - Schedule 2 – Abolition of disclosure powers
  - Schedule 3 – Exceptions to section 48
  - Schedule 4 – Relevant public authorities and designated senior officers
    - Part 1 – Table of authorities and officers
    - Part 2 – Interpretation of table
  - Schedule 5 – Transfer and agency arrangements with public authorities: further provisions
  - Schedule 6 – Issue of warrants under section 96 etc: table
    - Part 1 – Table: Part 1
    - Part 2 – Table: Part 2
    - Part 3 – Interpretation of the table
  - Schedule 7 – Codes of practice
  - Schedule 8 – Combination of warrants and authorisations
    - Part 1 – Combinations with targeted interception warrants
    - Part 2 – Other combinations involving targeted equipment interference warrants
    - Part 3 – Combinations involving targeted examination warrants only
    - Part 4 – Combined warrants: supplementary provision
  - Schedule 9 – Transitional, transitory and saving provision
  - Schedule 10 – Minor and consequential provision
    - Part 1 – General amendments
    - Part 2 – Lawful interception of communications
    - Part 3 – Acquisition of communications data
    - Part 4 – Retention of communications data
    - Part 5 – Equipment interference
    - Part 6 – Judicial Commissioners
    - Part 7 – Other minor and consequential provision
    - Part 8 – Repeals and revocations consequential on other repeals or amendments in this Act

A  
**B I L L**

TO

Make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.

**B**E IT ENACTED by the Queen’s most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

**PART 1**

GENERAL PRIVACY PROTECTIONS

*Overview of Act*

**1 Overview of Act**

- (1) This Part sets out offences and penalties in relation to— 5
  - (a) the unlawful interception of communications, and
  - (b) the unlawful obtaining of communications data.
- (2) It 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. 10
- (3) Other 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 by virtue of the Human Rights Act 1998 and elsewhere in the law.
- (4) The regimes provided for by Parts 2 to 7 are as follows –
- (a) Part 2 and Chapter 1 of Part 6 set out circumstances 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, 5
  - (b) Part 3 and Chapter 2 of Part 6 set out circumstances in which the obtaining of communications data is lawful and make further provision about the obtaining and treatment of such data, 10
  - (c) Part 4 makes provision for the retention of certain communications data,
  - (d) Part 5 and Chapter 3 of Part 6 deal with equipment interference warrants, and
  - (e) Part 7 deals with bulk personal dataset warrants. 15
- (5) 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. 20

*Prohibitions against unlawful interception*

**2 Offence of unlawful interception**

- (1) A person commits an offence if – 25
- (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, 30
  - (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 – 35
- (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 3 and 4 contain provision about –
- (a) the meaning of “interception”, and 40
  - (b) when interception is to be regarded as carried out in the United Kingdom.
- (4) Section 5 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 223 and 224.  |    |
| (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;  | 5  |
|          | (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—  | 10 |
|          | (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.  |    |
| <b>3</b> | <b>Definition of “interception” etc.</b>   | 15 |
|          | <i>Interception in relation to telecommunication systems</i>   |    |
| (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.  | 20 |
|          | For the meaning of “content” in relation to a communication, see section 223(6).   |    |
| (2)      | In this section “relevant act”, in relation to a telecommunication system, means—  | 25 |
|          | (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—  | 30 |
|          | (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.   | 35 |
| (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).  | 40 |
| (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. | 45 |

- (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. 5

*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 – 10
- (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 – 15
    - (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. 20

#### 4 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. 25
- (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 30
  - (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. 35

For the meaning of “postal data”, see section 224.

#### 5 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 – 40
- (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 37 to 45, or 45



- (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, 5
  - (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. 10
- (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 15
  - (b) is authorised by any of sections 37 to 45, is to be treated as lawful for all purposes.

## 6 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. 20
- (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 – 25
  - (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 30
  - (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 2. 35
- (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 – 40
  - (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 3 to 5. 45

|          |   |    |
|----------|---|----|
| <b>7</b> | <b>Restriction on requesting interception by overseas authorities</b>   |    |
| (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.   | 5  |
| (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   | 10 |
|          | (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.  |    |
| <b>8</b> | <b>Restriction on requesting assistance under mutual assistance agreements etc.</b>   | 15 |
| (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. | 20 |
| (3)      | In this section—  |    |
|          | “EU mutual assistance instrument” means an EU instrument which—   | 25 |
|          | (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;  | 30 |
|          | “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,  | 35 |
|          | (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.  |    |
|          | <i>Prohibition against unlawful obtaining of communications data</i>  | 40 |
| <b>9</b> | <b>Offence of unlawfully obtaining communications data</b>  |    |
| (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. 5
- (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 10
    - (ii) to a fine,or to both;
  - (b) on summary conviction in Scotland –
    - (i) to imprisonment for a term not exceeding 12 months, or 15
    - (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, 20or to both;
  - (d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

*Abolition of powers to obtain communications data*

- 10 Abolition or restriction of certain powers to obtain communications data 25**
- (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 – 30
- (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 35
- 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. 40
- (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 for the purpose of regulatory functions,
  - “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*

## 11 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 5
    - (iii) equipment data which forms part of, or is connected with, communications or private information falling within subparagraph (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 – 10
    - (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 15
    - (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 118);
    - “equipment interference warrant” means – 20
      - (a) a targeted equipment interference warrant under Part 5;
      - (b) a bulk equipment interference warrant under Chapter 3 of Part 6.
- 12 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 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). 25 30
  - (2) In this section, “communications”, “private information” and “equipment data” have the same meaning as in Part 5 (see section 118).

## PART 2

### LAWFUL INTERCEPTION OF COMMUNICATIONS 35

#### CHAPTER 1

##### INTERCEPTION AND EXAMINATION WITH A WARRANT

###### *Warrants under this Chapter*

### 13 Warrants that may be issued under this Chapter

- (1) There are three kinds of warrant that may be issued under this Chapter – 40
  - (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— 5
- (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 14); 10
  - (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 134(4) (prohibition on seeking to identify communications of individuals in the British Islands). 15
- 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. 20
- (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— 25
- (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; 30
  - (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. 35
- (5) A targeted interception warrant or mutual assistance warrant also authorises the following conduct (in addition to the conduct described in the warrant)— 40
- (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; 45
  - (c) any conduct for obtaining related systems data from any postal operator or telecommunications operator. 50



- (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 5  
“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. 10
- (7) For provision enabling the combination of targeted interception warrants with certain other warrants or authorisations (including targeted examination warrants), see Schedule 8.

**14 Obtaining secondary data** 15

- (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 3(7)). 20
- (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). 25
- (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). 30
- (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). 35
- (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 40  
(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. 45
- (7) For the meaning of “systems data” and “identifying data”, see section 225.

## 15 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; 5
  - (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; 10
  - (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 15
    - (ii) the training of persons who carry out, or are likely to carry out, such interception or the obtaining of such data; 20
  - (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 25
    - (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*

## 16 Persons who may apply for issue of a warrant 30

- (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; 35
  - (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. 40
- (2) For the meaning of “head of an intelligence service”, see section 225.



- (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.

## 17 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 16(1)(a) to (g), issue a targeted interception warrant if – 5
- (a) the Secretary of State considers that the warrant is necessary on grounds falling within section 18,
  - (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, 10
  - (c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 46 and 47 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and 15
  - (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 (5).

- (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 – 20
- (a) the Secretary of State considers that the warrant is necessary on grounds falling within section 18,
  - (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, 25
  - (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 134(4) (prohibition on seeking to identify communications of individuals in the British Islands), and 30
  - (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 (5).

- (3) The Secretary of State may, on an application made by or on behalf of an intercepting authority, issue a mutual assistance warrant if – 35
- (a) the Secretary of State considers that the warrant is necessary on grounds falling within section 18,
  - (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, 40
  - (c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 46 and 47 (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. 45

This is subject to subsection (5).

- (4) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) or (as the case may be) subsection (3) are met include whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means.
- (5) The Secretary of State may not issue a warrant under this section if – 5
- (a) the application is a relevant Scottish application (see section 20), 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. 10
- For the power of the Scottish Ministers to issue warrants under this Chapter, see section 19.
- (6) But subsection (5) 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. 15

## **18 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 – 20
- (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 – 25
- (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). 30
- (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. 35
- (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.

## **19 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 16(1)(a) to (g), issue a targeted interception warrant if – 40
- (a) the application is a relevant Scottish application (see section 20),
  - (b) the Scottish Ministers consider that the warrant is necessary on grounds falling within subsection (4), 45

- (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 46 and 47 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and 5
  - (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 – 10
  - (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, 15
  - (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 134(4) (prohibition on seeking to identify communications of individuals in the British Islands), and 20
  - (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 – 25
  - (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, 30
  - (d) the Scottish Ministers consider that satisfactory arrangements made for the purposes of sections 46 and 47 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and 35
  - (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 – 40
  - (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 45
    - (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 matters to be taken into account in considering whether the conditions in paragraphs (b) and (c) of subsection (1) or (as the case may be) subsection (3) are met include whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means. 5

## 20 “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. 10  
 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 15
  - (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 20
    - (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— 25
    - (i) the making of a request falling within section 13(4)(a), or
    - (ii) the making of such a request and disclosure falling within section 13(4)(c), and
  - (b) the application—
    - (i) is made by, or on behalf of, the chief constable of the Police Service of Scotland, or 30
    - (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. 35
- (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 13(4)(b), or 40
    - (ii) the provision of such assistance and disclosure falling within section 13(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 45
    - (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*

**21 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 – 5
  - (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 apply the same principles as would be applied by a court on an application for judicial review. 10
- (3) In subsection (1)(a) “relevant grounds” means –
  - (a) in the case of a warrant to be issued by the Secretary of State, grounds falling within section 18;
  - (b) in the case of a warrant to be issued by the Scottish Ministers, grounds falling within section 19(4). 15
- (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. 20

**22 Approval of warrants issued in urgent cases**

- (1) This section applies where – 25
  - (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. 30
- (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. 35
- (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. 40
- (5) Section 23 contains further provision about what happens if a Judicial Commissioner refuses to approve the decision to issue a warrant.

### **23 Failure to approve warrant issued in urgent case**

- (1) This section applies where under section 22(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. 5
- (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. 10
- (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 15
  - (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) – 20
  - (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). 25
- (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 22 affects the lawfulness of – 30
  - (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. 35

*Additional safeguards*

### **24 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 40
  - (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. 5
  - (2) Before deciding whether to issue the warrant, the Secretary of State must consult the Prime Minister.
  - (3) In this section “member of a relevant legislature” means –
    - (a) a member of either House of Parliament; 10
    - (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.
- 25 Items subject to legal privilege 15**
  - (1) Subsections (2) and (3) 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 20
      - (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. 25
  - (3) 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 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 46 or (as the case may be) section 132 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of such items. 30 35
  - (4) Subsections (5) and (6) apply if –
    - (a) an application is made by or on behalf of an intercepting authority for a warrant under this Chapter, 40
    - (b) the intercepting authority considers that the relevant communications are likely to include items subject to legal privilege, and
    - (c) subsections (2) and (3) do not apply.
  - (5) The application must contain – 45

- (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. 5
- (6) 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 46 or (as the case may be) section 132 include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege.
- (7) In this section “relevant communications” means – 10
- (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. 15

*Further provision about warrants*

**26 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 – 20
- (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 – 25
- (a) subsection (4), and
  - (b) section 33 (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. 30
- (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. 35
- (6) In this section “senior official” means – 40
- (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.



## 27 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. 5
- (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 – 10
  - (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 – 15
  - (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. 20
- (6) A warrant that relates to any testing or training activities must – 25
  - (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 15(3).
- (7) A person is within this subsection if – 30
  - (a) in the case of a targeted interception warrant, communications from, or intended for, the person will or may be intercepted by an interception authorised or required by the warrant, or
  - (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 – 35
  - (a) a targeted interception warrant or mutual assistance warrant authorises or requires the interception of communications described in the warrant, or
  - (b) a targeted examination warrant authorises the selection of the content of communications for examination, 40the 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 – 45
  - (a) communications from, or intended for, any person named or described in the warrant, or

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

## 28 Duration of warrants

- (1) A warrant under this Chapter ceases to have effect at the end of the relevant period (see subsection (2)), unless – 5
- (a) it is renewed before the end of that period (see section 29), or
- (b) it is cancelled or otherwise ceases to have effect before the end of that period (see sections 22 and 32).
- (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; 10
- (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. 15
- (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 20
- (b) the person who decided to issue the warrant considered that there was an urgent need to issue it.

## 29 Renewal of warrants

- (1) If the renewal conditions are met, a warrant issued under this Chapter may be renewed, at any time before the end of the relevant period, by an instrument issued by the appropriate person (see subsection (3)). 25
- (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, 30
- (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 134(4), and 35
- (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; 40
- (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 18;
    - (b) in the case of a warrant issued by the Scottish Ministers, grounds falling within section 19(4).
  - (5) 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. 5
  - (6) Section 21 (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). 10
  - (7) Sections 24 (Members of Parliament etc.) and 25 (items subject to legal privilege) apply in relation to a decision to renew a warrant as they apply in relation to a decision to issue a warrant. 15
  - (8) In this section “the relevant period” has the same meaning as in section 28.
  - (9) This section is subject to section 33 (special rules for certain mutual assistance warrants).
- 30 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. 20
  - (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 27(8). 25
  - (3) 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.
  - (4) In this section –
    - (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”. 30
  - (5) 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. 40
  - (6) A minor modification may be made by –
    - (a) the Secretary of State, in the case of a warrant issued by the Secretary of State, 45

- (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 5
- (e) a person who holds a senior position in the same public authority as the person mentioned in paragraph (d).
- (7) But if a person within subsection (6)(d) or (e) considers that there is an urgent need to make a major modification, that person (as well as a person within subsection (5)) may do so. 10  
 Section 31 contains provision about the approval of major modifications made in urgent cases.
- (8) For the purposes of subsection (6)(e) a person holds a senior position in a public authority if— 15
- (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; 20
- (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; 25
- (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. 30
- (9) A person may make a major modification of a warrant by adding a name or description as mentioned in subsection (2)(a) only if the person considers—
- (a) that the modification is necessary on any relevant grounds (see subsection (10)), and 35
- (b) that the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct.
- (10) In subsection (9)(a) “relevant grounds” means—
- (a) in the case of a warrant issued by the Secretary of State, grounds falling within section 18; 40
- (b) in the case of a warrant issued by the Scottish Ministers, grounds falling within section 19(4);
- and for the purposes of subsection (9) any reference to the Secretary of State in section 18(3)(b) or the Scottish Ministers in section 19(4)(b) is to be read as a reference to the person making the modification. 45
- (11) Sections 24 (Members of Parliament etc.) and 25 (items subject to legal privilege) apply in relation to a decision to make a major modification of a warrant by adding a name or description as mentioned in subsection (2)(a) as

they apply in relation to a decision to issue a warrant; and accordingly where section 24 applies only the Secretary of State may make the modification.

- (12) Where a major modification of a warrant is made by a senior official in accordance with subsection (5), 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. 5
- (13) If at any time a person mentioned in subsection (6) considers that any factor specified in a warrant in accordance with section 27(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 27(9)(a) or (b), the person must modify the warrant by removing that factor. 10
- (14) 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; 15  
(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.
- (15) 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. 20

### 31 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 30(7).
- (2) The person who made the modification must inform a designated senior official that it has been made. 25
- (3) In this section –  
“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 30  
“senior official” has the same meaning as in section 30.
- (4) In addition, 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. 35
- (5) The designated senior official 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 senior official’s decision.  
“The relevant period” means the period ending with the fifth working day after the day on which the modification was made. 40
- (6) If the designated senior official refuses to approve the decision to make the modification –  
(a) 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 refusal, 45

- (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. 5
- (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 – 10
    - (i) anything done before that thing could be stopped, or
    - (ii) anything done which it is not reasonably practicable to stop.
- 32 Cancellation of warrants**
- (1) Any of the appropriate persons may cancel a warrant issued under this Chapter at any time. 15
- (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, 20
- 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 18; 25
  - (b) in the case of a warrant issued by the Scottish Ministers, grounds falling within section 19(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; 30
  - (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. 35
- (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; 40
  - (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. 45



- (8) See also section 33 (which imposes a duty to cancel mutual assistance warrants in certain circumstances).

### 33 Special rules for certain mutual assistance warrants

- (1) For the purposes of this section a warrant is a “relevant mutual assistance warrant” if— 5
- (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— 10
    - (i) it appears that the interception subject is outside the United Kingdom, or
    - (ii) the interception to which the warrant relates 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. 15
- (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 20
  - (b) whichever of the following statements is applicable—
    - (i) a statement that the interception subject appears to be outside the United Kingdom; 25
    - (ii) a statement that the interception to which the warrant relates 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 29 to the appropriate person include, in the case of such a warrant, references to that senior official. 30
- (5) Where a senior official renews a relevant mutual assistance warrant in accordance with subsection (4), the instrument renewing the warrant must contain— 35
- (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 40
  - (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 to which the warrant relates is to take place in relation only to premises outside the United Kingdom. 45
- (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). 5
- (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 32. 10
- (8) In this section –
- “the interception subject”, in relation to a warrant, means the person, group of persons or organisation about whose communications information is sought by the interception to which the warrant relates; 15
  - “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*

- 34 Implementation of warrants** 20
- (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. 25
  - (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. 30
  - (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. 35
  - (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. 40
  - (6) References in this section and sections 35 and 36 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.

### **35 Service of warrants outside the United Kingdom**

- (1) This section applies to the service of warrants under section 34(3) on a person outside the United Kingdom. 5
- (2) A copy of a warrant may be served on the person 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; 10
  - (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; 15
  - (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 (3)).
- (3) A copy of a warrant may be served on a person in the way mentioned in subsection (2)(c) only if – 20
  - (a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (2)(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. 25
- (4) The steps mentioned in subsection (3)(b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.
- (5) In this section “the intercepting authority” has the same meaning as in section 34. 30

### **36 Duty of operators to assist with implementation**

- (1) A relevant operator that has been served with a copy of a warrant to which section 34 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. 35  
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 34. 40
- (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 5
  - (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 217 (maintenance of technical capability), 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. 10
- (7) A person who knowingly fails to comply with subsection (1) is guilty of an offence and liable— 15
- (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 20
    - (ii) to a fine,
 or to both;
  - (b) on summary conviction in Scotland—
    - (i) to imprisonment for a term not exceeding 12 months, or 25
    - (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, 30
 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. 35

## CHAPTER 2

### OTHER FORMS OF LAWFUL INTERCEPTION

#### *Interception with consent*

40

### 37 **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).

5

*Interception for administrative or enforcement purposes*

**38 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.

10

15

20

25

30

**39 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.

35

40

- 
- (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. 5
- (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, 10
  - (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.
- 40 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 – 15
- (a) section 105 of the Postal Services Act 2000 (power to open postal items etc.), or 20
  - (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).
- 41 Interception by OFCOM in connection with wireless telegraphy** 25
- (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; 30
  - (b) the obtaining, by or in connection with the interception, of information about the sender or recipient, or intended recipient, of the communication;
  - (c) the disclosure of anything obtained by conduct falling within paragraph (a) or (b). 35
- (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; 40
  - (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. 45

- (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; 5
  - “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*

**42 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. 10
- (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. 15
- (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 20
  - (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, 25
- 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. 30

**43 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. 35
- (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. 40
- (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). 5
- (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 10
- (b) section 284 of that Act (powers relating to the use of telephones by certain persons detained in hospital).
- (5) In this section – 15
- “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. 20
- 44 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 – 25
- “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; 30
- “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; 35
- (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*

- 45 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 C are met. 40
- (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. 5  
In this subsection “relevant international agreement” means an international agreement to which the United Kingdom is a party.
- (4) Condition C is that any further conditions specified in regulations made by the Secretary of State for the purposes of this section are met.

### CHAPTER 3

10

#### OTHER PROVISIONS ABOUT INTERCEPTION

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

#### 46 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. 15  
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)) – 20
  - (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; 25
  - (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 – 30
  - (a) it is, or is likely to become, necessary on any of the grounds falling within section 18 on which a warrant under Chapter 1 of this Part may be necessary, 30
  - (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, 35
  - (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 40
  - (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
- (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 – 10
- (a) its retention is not necessary, or not likely to become necessary, on any of the grounds falling within section 18 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. 15
- (7) Where an item subject to legal privilege intercepted in accordance with a targeted interception warrant or mutual assistance warrant is retained following its examination, the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable. 20
- (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. 25
- (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 47).
- (10) In this section – 30
- “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 – 35
      - (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; 40
  - “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; 45  - “overseas authorities” means authorities of a country or territory outside the United Kingdom.

#### 47 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 5
  - (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 46(2) and (5) (“the relevant requirements”) 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 10
  - (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. 15
- (3) In subsection (2)(b) “prohibited disclosure” means a disclosure which, if made in the United Kingdom, would breach the prohibition in section 48(1). 20
- (4) In this section—
- “copy” has the same meaning as in section 46;
  - “the issuing authority” means— 25
    - (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. 30

#### 48 Exclusion of matters from legal proceedings

- (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— 35
    - (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. 40
- 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 2(1) (offence of unlawful interception); 45

- 
- (b) a breach of the prohibition imposed by section 7 (restriction on requesting interception by overseas authorities);
- (c) a breach of the prohibition imposed by section 8 (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; 5
- (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— 10
- (a) any person who is an intercepting authority (see section 16);
- (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; 15
- (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— 20
- (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); 25
- (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; 30
- (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— 35
- (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. 40
- (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. 45

#### 49 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 50).
- (3) This section applies to the following persons –
- (a) any person who is an intercepting authority (see section 16);
  - (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.

#### 50 Section 49: meaning of “excepted disclosure”

- (1) For the purposes of section 49 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 advisers);
  - (d) subsection (7) (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 34(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) 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; 5
  - (c) a disclosure made to the Independent Police Complaints Commission for the purposes of facilitating the carrying out of any of its functions.
- (4) 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;10
  - (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 (6)).15
- (5) But a disclosure within Head 3 is not an excepted disclosure if it is made with a view to furthering any criminal purpose. 20
- (6) In subsection (4)(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. 25
- (7) 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) relates to the number of warrants under Chapter 1 of this Part to which the operator has given effect or has been involved in giving effect;30
  - (b) a disclosure of information that does not relate to any particular warrant under Chapter 1 of this Part but relates to such warrants in general. 35
- (8) Nothing in this section affects the operation of section 48 (which, among other things, prohibits the making of certain disclosures in, for the purposes of or in connection with legal proceedings).
- 51 Offence of making unauthorised disclosures** 40
- (1) A person who fails to comply with section 49(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 the45

- 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 – 5
- (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 – 10
- (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. 15

### *Interpretation*

- 52 Part 2: interpretation** 20
- (1) In this Part –
- “EU mutual assistance instrument” has the meaning given by section 8(3);
  - “intercepting authority” is to be read in accordance with section 16;
  - “international mutual assistance agreement” has the meaning given by section 8(3); 25
  - “mutual assistance warrant” has the meaning given by section 13(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; 30
    - (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; 35
    - (h) the Royal Military Police;
    - (i) the Royal Air Force Police;
    - (j) the British Transport Police;
  - “relevant content”, in relation to a targeted examination warrant, has the meaning given by section 13(3); 40
  - “relevant Scottish application” has the meaning given by section 20;
  - “secondary data” has the meaning given by section 14, 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 13(3). 45



- (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 – 5  
 section 223 (telecommunications definitions),  
 section 224 (postal definitions),  
 section 225 (general definitions),  
 section 226 (index of defined expressions).

### PART 3 10

#### AUTHORISATIONS FOR OBTAINING COMMUNICATIONS DATA

##### *Targeted authorisations for obtaining data*

### 53 Power to grant authorisations

- (1) Subsection (2) applies if a designated senior officer of a relevant public authority considers – 15  
 (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 – 20  
     (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. 25
- (2) The designated senior officer may authorise any officer of the authority to engage in any conduct which – 30  
 (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 – 35  
 (a) section 54 (additional restrictions on grant of authorisations),  
 (b) sections 61 and 64 to 66 and Schedule 4 (restrictions relating to certain relevant public authorities),  
 (c) section 67 (requirement to consult a single point of contact), and  
 (d) section 68 (Commissioner approval for authorisations to identify or confirm journalistic sources).
- (4) Authorised conduct may, in particular, consist of an authorised officer – 40  
 (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 to disclose it to a person identified by, or in accordance with, the authorisation,



- (c) asking any person whom the authorised officer believes is not in possession of the communications data but is capable of obtaining it, to obtain it and disclose it to a person identified by, or in accordance with, the authorisation, or
- (d) requiring by notice a telecommunications operator – 5
  - (i) whom the authorised officer believes is, or may be, in possession of the communications data to disclose the data to a person identified by, or in accordance with, the authorisation, or
  - (ii) whom the authorised officer believes is not in possession of the communications data but is capable of obtaining the data, to obtain it and disclose it to a person identified by, or in accordance with, the authorisation. 10
- (5) An authorisation – 15
  - (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 20
  - (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 – 25
  - (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), (c) or (d), a person to disclose the data to any person other than – 30
    - (i) an authorised officer, or
    - (ii) an officer of the same relevant public authority as an authorised officer.
- (7) It is necessary and proportionate to obtain communications data for a purpose falling within this subsection if it is necessary and proportionate to obtain the data – 35
  - (a) in the interests of national security,
  - (b) for the purpose of preventing or detecting crime or of preventing disorder, 40
  - (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, 45
  - (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) See –
- (a) sections 61 and 64 for the meanings of “designated senior officer” and “relevant public authority”;
  - (b) section 75 for the way in which this Part applies to postal operators and postal services.
- 54 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 interests of national security, or
    - (c) the size of the relevant public authority concerned being such that it is not practicable to have a designated senior officer who is not working on the investigation or operation concerned.
  - (4) 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 the purpose of obtaining the data is to identify –
    - (a) which person or apparatus is using an internet service where –
      - (i) the service and time of use are already known, but
      - (ii) the identity of the person or apparatus using the service is not known,
    - (b) 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,
    - (c) 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

- (d) 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) 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. 5
- (6) 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 10
  - (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).

## 55 Procedure for authorisations and authorised notices

- (1) An authorisation must specify— 15
  - (a) the office, rank or position held by the designated senior officer granting it,
  - (b) the matters falling within section 53(7) by reference to which it is granted,
  - (c) the conduct that is authorised, 20
  - (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— 25
  - (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— 30
    - (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. 35
- (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.

## 56 Duration and cancellation of authorisations and notices 40

- (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 must cancel it if the designated senior officer considers that the position is no longer as mentioned in section 53(1)(a), (b) or (c). 5
- (5) The Secretary of State may by regulations provide for the person by whom any duty imposed by subsection (4) is to be performed in a case in which it would otherwise fall on a person who is no longer available to perform it. 10
- (6) Such regulations may, in particular, provide for the person on whom the duty is to fall 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) – 15
- (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).

## 57 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. 20
- (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. 25
- (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 217 (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. 30
- (5) The duty imposed by subsection (1) or (2) is enforceable by the Secretary of State by civil proceedings 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. 35

### *Filtering arrangements for obtaining data*

## 58 Filtering arrangements for obtaining data 40

- (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 position is as mentioned in section 53(1)(a), (b) and (c), or
  - (b) facilitating the lawful, efficient and effective obtaining of communications data from any person by relevant public authorities in pursuance of an authorisation. 5
- (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 10
  - (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 15
    - (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 – 20
  - (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). 25
- (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 196(1) of keeping under review the exercise by public authorities of functions under this Part. 30
- (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). 35

## 59 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, 40
  - (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). 45
- (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, 5
  - (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, 10
- unless the condition in subsection (5) is met.
- (5) The condition is that the designated senior officer (as well as considering that the position is as mentioned in section 53(1)(a), (b) and (c)) considers that what is authorised in relation to the filtering arrangements is proportionate to what is sought to be achieved. 15

## 60 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 – 20
    - (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 58(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, 25
  - (c) that any authorisation data which is obtained under the filtering arrangements in pursuance of an authorisation is immediately destroyed – 30
    - (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 – 35
- (a) for the purpose mentioned in section 58(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 58(4) or (5), or 40
  - (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 45



- (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 58(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
  - (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 10
    - (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 15
    - (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. 20
  - (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. 25
  - (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* 30

## 61 Relevant public authorities and designated senior officers

- (1) Schedule 4 (relevant public authorities and designated senior officers) 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. 35
- (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 40
  - (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
- (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— 10
- (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 53(1)(a) is met in relation to a purpose within one of the paragraphs of section 53(7) specified in the corresponding entry in column 4 of the table. 15
- (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. 20

## 62 Power to modify section 61 and Schedule 4

- (1) The Secretary of State may by regulations modify section 61 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, 25
  - (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. 30
- (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. 35

## 63 Certain regulations under section 62: supplementary

- (1) This section applies to regulations under section 62 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, 40
  - (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. 45

- (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. 5

*Local authorities*

**64 Local authorities as relevant public authorities**

- (1) A local authority is a relevant public authority for the purposes of this Part. 10
- (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. 15
- (3) A designated senior officer of a local authority may grant an authorisation for obtaining communications data only if section 53(1)(a) is met in relation to a purpose within section 53(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. 20
- (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. 25
- (7) Sections 65 and 66 impose further restrictions in relation to the grant of authorisations by local authorities.

**65 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 70(6) and (7)) as being appropriate for the local authority. 35
- (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. 40

- (4) If a local authority is itself a supplying authority under a collaboration agreement, 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 69. 5

## 66 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 68 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. 10
- (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. 15
- (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 20  
 (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. 25
- (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 30  
 (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). 35

### *Additional protections*

## 67 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. 40

- (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 5
  - (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 10
    - (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 – 15
  - (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 – 20
    - (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 25
  - (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, 30
  - (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, 35
  - (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, 40
  - (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.

**68 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 5
  - (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 made an order under this section approving it. 10
- (3) The relevant public authority for which the authorisation has been granted may apply to a Judicial Commissioner for an order under this section approving the authorisation.
- (4) The applicant is not required to give notice of the application to—
- (a) any person to whom the authorisation relates, or 15
  - (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 20
  - (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. 25
- (6) Where, on an application under this section, the Judicial Commissioner refuses to approve the grant of the authorisation, the Judicial Commissioner may make an order quashing the authorisation.
- (7) In this Act “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. 30

*Collaboration agreements***69 Collaboration agreements**

- (1) A collaboration agreement is an agreement (other than a police collaboration agreement) under which— 35
- (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 40
  - (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. 5
  - (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). 10
  - (3) In a case falling within subsection (1)(b)(i) –
    - (a) section 53 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, and 15
    - (b) section 54(3)(c) has effect as if the reference to the relevant public authority concerned were a reference to both authorities.
  - (4) In a case falling within subsection (1)(b)(ii) – 20
    - (a) section 53 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 25
    - (b) section 54(3)(c) 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 67(4)(b) has effect as if the references to the relevant public authority were references to the subscribing authority. 30
  - (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, 35
    - “police collaboration agreement” means a collaboration agreement under section 22A of the Police Act 1996 which contains force collaboration provision.
- 70 Collaboration agreements: supplementary**
- (1) A collaboration agreement may provide for payments to be made between parties to the agreement. 40
  - (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. 45
  - (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
- (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. 10
- (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. 15

## 71 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, and
  - (b) under the terms of the agreement – 20
    - (i) a designated senior officer of force 1 is permitted to grant authorisations to officers of a collaborating police force,
    - (ii) officers of force 1 are permitted to be granted authorisations by a designated senior officer of a collaborating police force, or
    - (iii) officers of force 1 act as single points of contact for officers of a collaborating police force. 25
- (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). 30
- (3) In a case falling within subsection (1)(b)(i) –
- (a) section 53 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 35
    - (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, and
  - (b) section 54(3)(c) has effect as if the reference to the relevant public authority concerned were a reference to force 1 and the collaborating police force. 40
- (4) In a case falling within subsection (1)(b)(ii) –
- (a) section 53 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 45



- (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 54(3)(c) has effect as if the reference to the relevant public authority concerned were a reference to force 1 and the collaborating police force. 5
- (5) In a case falling within subsection (1)(b)(iii), section 67(4)(b) has effect as if the references to the relevant public authority were references to the collaborating police force.
- (6) In this section – 10
  - “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 – 15
    - (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 69 (see subsection (6) of that section), 20and 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*

- 72 Lawfulness of conduct authorised by this Part** 25
- (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. 30
  - (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 35
    - (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. 40
  - (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 45

- (d) section 5 of the Intelligence Services Act 1994 (warrants for the intelligence services).

### 73 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.

### 74 Certain transfer and agency arrangements with public authorities

- (1) The Secretary of State may by regulations provide for –
- (a) any function under sections 58 to 60 which is exercisable by the Secretary of State to be exercisable instead by another public authority, or
- (b) any function under sections 58 to 60 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. 5

## 75 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 – 10
  - (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, 15
  - (d) in section 54, subsections (4) to (6) 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 224(3)”. 20

## 76 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. 25
- (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, 30
  - (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, 35
  - (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 57 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 – 40

- (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 57(1) or (2), may apply. 5

## 77 Part 3: interpretation

- (1) In this Part – 10
- “authorisation” means an authorisation under section 53 (including that section as modified by sections 69 and 71),
  - “designated senior officer” –
    - (a) in relation to a relevant public authority which is a local authority, has the meaning given by section 64(2), and 15
    - (b) in relation to any other relevant public authority, has the meaning given by section 61(3),
  - “filtering arrangements” means any arrangements under section 58(1),
  - “officer”, in relation to a relevant public authority, means a person holding an office, rank or position with that authority, 20
  - “relevant public authority” means a public authority which is a relevant public authority for the purposes of this Part by virtue of section 61(2) or 64(1).
- (2) In this Part “local authority” means – 25
- (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, 30
  - (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 – 35
- section 223 (telecommunications definitions),
  - section 224 (postal definitions),
  - section 225 (general definitions),
  - section 226 (index of defined expressions).

## PART 4

### RETENTION OF COMMUNICATIONS DATA

#### *General*

#### **78 Powers to require retention of certain data**

- (1) The Secretary of State may by notice (a “retention notice”) require a telecommunications operator to retain relevant communications data if 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 53(7) (purposes for which communications data may be obtained). 5
- (2) A retention notice may – 10
  - (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, 15
  - (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 – 20
  - (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 223(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 25
  - (c) in any other case, the day on which the data is first held by the operator concerned.
- (4) 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. 30
- (5) A retention notice comes into force –
  - (a) when the notice is given to the operator (or description of operators) concerned, or 35
  - (b) (if later) at the time or times specified in the notice.
- (6) 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. 40
- (7) 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 213(7) (the level or levels of contribution in respect of costs incurred as a result of the notice).
- (8) The requirements or restrictions mentioned in subsection (7)(d) may, in particular, include— 5
- (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— 10
    - (i) data for retention, or
    - (ii) retained data.
- (9) In this Part “relevant communications data” means communications data which may be used to identify, or assist in identifying, any of the following— 15
- (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 20
  - (e) the location of any such system,
- and this expression therefore includes, in particular, internet connection records.

### *Safeguards*

- 79 Matters to be taken into account before giving retention notices** 25
- (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, 30
  - (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. 35
- 80 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. 40
- (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
  - (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 – 10
    - (a) the Technical Advisory Board, and
    - (b) the Investigatory Powers 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. 15
  - (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, 20
    - (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 – 25
    - (a) vary or revoke the retention notice under section 83, or
    - (b) give a notice under this section to the operator concerned confirming its effect.
  - (11) 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. 30
  - (12) The Secretary of State must keep a retention notice under review (whether or not referred under subsection (1)). 20
- 81 Data integrity and security** 35
- (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, 40
    - (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. 45



- (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. 5

## 82 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. 10

### *Variation or revocation of notices*

## 83 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. 15
- (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. 20
- (4) A retention notice may not be varied so as to require the retention of additional relevant communications data unless 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 53(7) (purposes for which communications data may be obtained). 25
- (5) Section 78(2) and (4) 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.
- (6) Sections 78(3) and (7), 84 and 86, and subsections (1), (4), (9) and (12) of this section, apply in relation to a retention notice as varied as they apply in relation to a retention notice. 30
- (7) Section 79 applies in relation to the making of a variation as it applies in relation to the giving of a retention notice.
- (8) Section 80 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. 35
- (9) The Secretary of State may revoke (whether wholly or in part) a retention notice.
- (10) 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 40

- revocation to the attention of the operator (or description of operators) to whom it relates.
- (11) A revocation comes into force—
- (a) when notice of it is given or published in accordance with subsection (10), or 5
  - (b) (if later) at the time or times specified in the notice of revocation.
- (12) 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). 10

### *Enforcement*

#### **84 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— 15
- (a) a retention notice, or
  - (b) section 81 or 82,
- 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. 20
- (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. 25
- (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. 30

### *Further and supplementary provision*

#### **85 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— 35
- (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, 40

- (d) in section 78(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 224(3), the day on which the person concerned leaves the postal service concerned or (if earlier) the day on which the data is changed,” and 5
- (e) in section 78(9), the words from “and this expression” to the end were omitted.
- 86 Extra-territorial application of Part 4** 10
- (1) A retention notice, and any requirement or restriction imposed by virtue of a retention notice or by section 81, 82 or 84(1) to (3), may relate to conduct outside the United Kingdom and persons outside the United Kingdom.
- (2) But section 84(5), so far as relating to those requirements or restrictions, does not apply to a person outside the United Kingdom. 15
- 87 Part 4: interpretation**
- (1) In this Part –  
     “notice” means notice in writing,  
     “relevant communications data” has the meaning given by section 78(9),  
     “retention notice” has the meaning given by section 78(1). 20
- (2) See also –  
     section 223 (telecommunications definitions),  
     section 224 (postal definitions),  
     section 225 (general definitions),  
     section 226 (index of defined expressions). 25

## PART 5

### EQUIPMENT INTERFERENCE

#### *Warrants under this Part*

- 88 Warrants under this Part: general** 30
- (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 – 35  
     (a) communications (see section 118);  
     (b) equipment data (see section 89);  
     (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). 5
- (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; 10
- (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; 15
- (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. 20
- (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 2(1) (unlawful interception). 25
- (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). 30
- (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 170(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands). 35
- 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 – 40
- (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. 45
- (11) Any conduct which is carried out in accordance with a warrant under this Part is lawful for all purposes.

**89 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 – 5
- (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 10
  - (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. 15
- (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 225.

**90 Subject-matter of warrants**

- (1) A targeted equipment interference warrant may relate to any one or more of the following matters – 20
- (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; 25
  - (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; 30
  - (e) equipment in more than one location, where the interference is for the purpose of the same 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; 35
  - (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. 40
- (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; 45
  - (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*

5

**91 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), 10
  - (b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by which conduct,
  - (c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 112 and 113 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and 15
  - (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— 20
  - (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. 25

For the power of the Scottish Ministers to issue a targeted equipment interference warrant, see section 92. 30
- (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, 35
  - (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 170(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands), and 40
  - (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. 45
- (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 92.

- (5) A warrant is necessary on grounds falling within this subsection if it is necessary – 5
- (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. 10
- (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. 15
- (7) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means.
- (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. 20
- (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. 25

## 92 Power to issue warrants to intelligences 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, 30
  - (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, 35
  - (d) the Scottish Ministers consider that satisfactory arrangements made for the purposes of sections 112 and 113 (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. 40
- (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, 45



- (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, 5
    - (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 170(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands), and 10
    - (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 matters to be taken into account in considering whether the conditions in paragraphs (b) and (c) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means. 15
  - (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.
- 93 Power to issue warrants to the Chief of Defence Intelligence 20**
- (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, 25
    - (c) the Secretary of State considers that satisfactory arrangements made for the purposes of section 112 and 113 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and 30
    - (d) except where the Secretary of State considers that there is an urgent need to issue a warrant, the decision to issue it has been approved by a Judicial Commissioner.
  - (2) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means. 35
  - (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.
- 94 Members of Parliament etc. 40**
- (1) This section 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 45

- (ii) a member of a relevant legislature’s private information.
- (2) This section 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) Before deciding whether to issue the warrant, the Secretary of State must consult the Prime Minister.
- (4) 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.
- 95 Decision to issue warrants under sections 91 to 93 to be taken personally by Ministers**
- (1) The decision to issue a warrant under section 91 or 93 must be taken personally by the Secretary of State.
- (2) The decision to issue a warrant under section 92 must be taken personally by a member of the Scottish Government.
- (3) Before a warrant under section 91, 92 or 93 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) the Scottish Ministers have personally and expressly authorised the issue of the warrant.
- 96 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 112 and 113 (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 it has been approved by a Judicial Commissioner. 5
- (2) 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, 10
  - (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, 15
  - (c) the law enforcement chief considers that satisfactory arrangements made for the purposes of sections 112 and 113 (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 it has been approved by a Judicial Commissioner. 20
- (3) 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. 25
- (4) 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; 30
  - (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.
- (5) 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. 35
- (6) 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). 40
- (7) 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. 45
- (8) 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.
- (9) 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. 5
- (10) 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. 10
- (11) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) or (2) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means. 15
- (12) For the purpose of subsection (6), 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 20
  - (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; 25
    - (iv) the British Nationality (Hong Kong) Act 1997;
    - (v) the British Overseas Territories Act 2002;
    - (vi) an instrument made under any of those Acts.
- (13) 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); 30
  - “immigration officer” means a person appointed as an immigration officer under paragraph 1 of Schedule 2 to the Immigration Act 1971.

*Approval of warrants by Judicial Commissioners* 35

**97 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 40
  - (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 apply the same principles as would be applied by a court on an application for judicial review.
- (3) In subsection (1)(a), “relevant grounds” means –
  - (a) in the case of a warrant to be issued under section 91, grounds falling within section 91(5); 5
  - (b) in the case of a warrant to be issued under section 92, the purpose of preventing or detecting serious crime;
  - (c) in the case of a warrant to be issued under section 93, the interests of national security;
  - (d) in the case of a warrant to be issued under section 96(1), the purpose mentioned in section 96(1)(a); 10
  - (e) in the case of a warrant to be issued under section 96(2), the purpose mentioned in section 96(2)(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. 15
- (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. 20

## **98 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. 25
- (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 30
  - (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. 35
- (5) Section 99 contains further provision about what happens if a Judicial Commissioner refuses to approve the decision to issue a warrant.

## **99 Failure to approve warrant issued in urgent case 40**

- (1) This section applies where under section 98(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 – 5
- (a) 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 stops as soon as possible;
  - (b) direct that any of the material obtained under the warrant is destroyed; 10
  - (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 – 15
- (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)). 20
- (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). 25
- (8) On a review under subsection (7), the Investigatory Powers Commissioner may –
- (a) confirm the Judicial Commissioner’s decision, or 30
  - (b) make a fresh determination.
- (9) Nothing in this section or section 98 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 – 35
    - (i) anything done before that thing could be stopped, or
    - (ii) anything done that it is not reasonably practicable to stop.

*Additional safeguards*

**100 Items subject to legal privilege**

- (1) Subsections (2) and (3) apply if – 40
- (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. 5
- (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. 10
- (3) 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 15
  - (b) that the arrangements made for the purposes of section 112 or (as the case may be) section 168 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of such items. 20
- (4) Subsections (5) and (6) 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 25
  - (c) subsections (2) and (3) do not apply.
- (5) 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. 30
- (6) 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 112 or (as the case may be) section 168 include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege. 35
- (7) 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. 40

*Further provision about warrants*

**101 Requirements which 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 – 45



- (a) in the case of a warrant issued under section 91 or 92, 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 93, to the Chief of Defence Intelligence; 5
- (c) in the case of a warrant issued under section 96 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 10
- (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.

| <i>Matter</i>  | <i>Details to be included in the warrant</i>  | 15 |
|--|---|----|
| 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   | 20 |
| 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                                       | 25 |
| 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 | 30 |
| Equipment in a particular location   | A description of the location   | 35 |
| 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   | 40 |

| <i>Matter</i>  | <i>Details to be included in the warrant</i>   |    |
|--|--|----|
| 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                                 | 5  |
| 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 | 10 |
| 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  | 15 |
| (4) A targeted equipment interference warrant must also describe—  |  |    |
| (a) the type of equipment which is to be interfered with, and  |  | 20 |
| (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. |  | 25 |

| <i>Matter</i>  | <i>Details to be included in the warrant</i>  |    |
|--|---|----|
| A particular person or organisation  | The name of the person or organisation or a description of the person or organisation   | 30 |
| 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                                       | 35 |
| 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 | 40 |

| <i>Matter</i>   | <i>Details to be included in the warrant</i>   |    |
|---|--|----|
| The testing, maintenance or development of capabilities relating to the selection or protected material for examination | A description of the nature of the testing, maintenance or development of capabilities | 5  |
| 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  | 10 |

## 102 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 – 15
- (a) it is renewed before the end of that period (see section 103), or
  - (b) it is cancelled or otherwise ceases to have effect before the end of that period (see sections 98 and 108).
- (2) In this section, “the relevant period” – 20
- (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 – 25
    - (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 – 30
- (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.

## 103 Renewal of warrants

- (1) If the renewal conditions are met, a warrant issued under this Part may be renewed, at any time before the end of the relevant period, by an instrument issued by the appropriate person (see subsection (3)). 35
- (2) The renewal conditions are – 40
- (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 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 170(4), and
- (d) that the decision to renew the warrant has been approved by a Judicial Commissioner.
- (3) The appropriate person is – 5
- (a) in the case of a warrant issued under section 91 or 93, the Secretary of State;
- (b) in the case of a warrant issued under section 92, a member of the Scottish Government;
- (c) in the case of a warrant issued under section 96 by a law enforcement chief or by an appropriate delegate in relation to the law enforcement chief, either – 10
- (i) the law enforcement chief, or
- (ii) if the warrant was issued by an appropriate delegate, that person. 15
- (4) In subsection (2)(a), “relevant grounds” means –
- (a) in the case of a warrant issued under section 91, grounds falling within section 91(5),
- (b) in the case of a warrant issued under section 92, the purpose of preventing or detecting serious crime, 20
- (c) in the case of a warrant issued under section 93, the interests of national security,
- (d) in the case of a warrant to be issued under section 96(1), the purpose mentioned in section 96(1)(a), or
- (e) in the case of a warrant to be issued under section 96(2), the purpose mentioned in section 96(2)(a). 25
- (5) The decision to renew a warrant issued under section 91 or 93 must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.
- (6) The decision to renew a warrant issued under section 92 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. 30
- (7) The instrument renewing a warrant issued under section 96 must be signed by the person who renews it.
- (8) Section 94 (Members of Parliament etc.) applies in relation to a decision to renew a warrant under this Part issued by the Secretary of State as it applies in relation to a decision to issue such a warrant. 35
- (9) Section 97 (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). 40
- (10) Section 100 (items subject to legal privilege) 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. 45
- (11) In this section, “relevant period” has the same meaning as in section 102.

**104 Modification of warrants issued by the Secretary of State or Scottish Ministers**

- (1) The provisions of a warrant issued under section 91, 92 or 93 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— 5
- (a) adding to the matters to which the warrant relates (see sections 90(1) and (2)), by including the details required in relation to that matter by section 101(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 101(3) or (5); 10
  - (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 101(3) or (5); 15
  - (e) adding to the descriptions of types of equipment included in the warrant in accordance with section 101(4)(a);
  - (f) varying or removing a description of a type of equipment included in the warrant in accordance with section 101(4)(a).
- (3) 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. 20
- (4) A modification may be made only if the person making the modification considers that—
- (a) the warrant as modified continues to be necessary on any relevant grounds (see subsection (5)), and 25
  - (b) the conduct authorised by the warrant as so modified is proportionate to what is sought to be achieved by that conduct.
- (5) In subsection (4)(a), “relevant grounds” means—
- (a) in the case of a warrant issued under section 91, grounds falling within section 91(5); 30
  - (b) in the case of a warrant issued under section 92, the purpose of preventing or detecting serious crime;
  - (c) in the case of a warrant issued under section 93, the interests of national security. 35
- (6) The persons who may make modifications under this section of a warrant are (subject to subsection (7))—
- (a) in the case of a warrant issued by the Secretary of State under section 91 or 93—
    - (i) the Secretary of State, 40
    - (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 92—
    - (i) a member of the Scottish Government, or
    - (ii) a senior official acting on behalf of the Scottish Ministers. 45
- (7) Any of the following persons may also make modifications under this section 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 105 contains provision about the approval of modifications made in urgent cases. 5
- (8) For the purposes of subsection (7)(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 10
    - (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 15
    - (ii) the person is of or above the rank of brigadier, commodore or air commodore.
- (9) Sections 94 (Members of Parliament etc.) applies in relation to a decision to make a modification of a warrant issued under section 91 or 93 which is of a kind described in subsection (2)(a), (c) or (e) as it applies in relation to a decision to issue such a warrant; and accordingly where that section applies only the Secretary of State may make the modification. 20
- (10) Section 100 (items subject to legal privilege) applies in relation to a decision to make a modification of a warrant issued under section 91, 92 or 93 which is of a kind described in subsection (2)(a), (c) or (e) as it applies in relation to a decision to issue such a warrant. 25
- (11) Where a senior official has made a modification of a warrant issued under section 91 or 93, the Secretary of State must be notified personally of the modification and the reasons for making it.
- (12) Where a senior official has made a modification of a warrant issued under section 92, a member of the Scottish Government must be notified personally of the modification and the reasons for making it. 30
- (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. 35
- 105 Approval of modifications under section 104 made in urgent cases**
- (1) This section applies where a person makes a modification of a warrant by virtue of section 104(7).
  - (2) The person who made the modification must inform a designated senior official that it has been made. 40
  - (3) In this section, “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.
  - (4) In addition, 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. 45



- (5) The designated senior official 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 senior official’s decision.
- “The relevant period” means the period ending with the fifth working day after the day on which the modification was made. 5
- (6) If the designated senior official refuses to approve the decision to make the modification –
- (a) 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 refusal, 10
  - (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. 15
- (7) In a case where a designated senior official refuses to approve a decision to make a modification of a targeted equipment interference warrant, the designated senior official 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. 20
- (8) If the designated senior official authorises further interference with equipment under subsection (7), 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. 25
- (9) 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 – 30
    - (i) anything done before that thing could be stopped, or
    - (ii) anything done which it is not reasonably practicable to stop.

## 106 Modification of warrants issued by law enforcement chiefs

- (1) The provisions of a warrant issued under section 96 by a law enforcement chief, or by an appropriate delegate in relation to that chief, may be modified at any time by – 35
- (a) 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 – 40
- (a) adding to the matters to which the warrant relates (see sections 90(1) and (2)), by including the details required in relation to that matter by section 101(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 101(3) or (5); 45



- (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 101(3) or (5);
  - (e) adding to the descriptions of types of equipment included in the warrant in accordance with section 101(4)(a); 5
  - (f) varying or removing a description of a type of equipment included in the warrant in accordance with section 101(4)(a).
- (3) A modification may be made only if—
- (a) the person making the modification considers that—
    - (i) the warrant as modified continues to be necessary on any relevant grounds (see subsection (4)), and 10
    - (ii) the conduct authorised by the warrant as so modified 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. 15
- (4) In subsection (3)(a), “relevant grounds” means—
- (a) in the case of a warrant to be issued under section 96(1), the purpose mentioned in section 96(1)(a); 20
  - (b) in the case of a warrant to be issued under section 96(2), the purpose mentioned in section 96(2)(a).
- (5) 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. 25
- (6) Section 97 (approval of warrants by Judicial Commissioners) applies in relation to a decision to make a modification of a warrant issued under section 96 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 warrant as modified, and 30
  - (b) any reference to the person who decided to issue the warrant were a reference to the person who decided to make the modification.
- (7) Section 100 (items subject to legal privilege) applies in relation to a decision to make a modification of a warrant issued under section 96 which is of a kind described in subsection (2)(a), (c) or (e) as it applies in relation to a decision to issue such a warrant. 35
- (8) 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.
- 107 Approval of modifications under section 106 in urgent cases 40**
- (1) This section applies where—
- (a) a modification is made under section 106 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. 45

- (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. 5
- “The relevant period” means the period ending with the fifth 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, 10
  - (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. 15
- (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. 20
- (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. 25
- (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 – 30
    - (i) anything done before that thing could be stopped, or
    - (ii) anything done which it is not reasonably practicable to stop.

## 108 Cancellation of warrants

- (1) Any of the appropriate persons may cancel a warrant issued under this Part at any time. 35
- (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, 40
- the person must cancel the warrant.
- (3) In subsection (2)(a), “relevant grounds” means –
- (a) in the case of a warrant issued under section 91, grounds falling within section 91(5);
  - (b) in the case of a warrant issued under section 92, the purpose of preventing or detecting serious crime; 45

- (c) in the case of a warrant issued under section 93, the interests of national security;
  - (d) in the case of a warrant to be issued under section 96(1), the purpose mentioned in section 96(1)(a);
  - (e) in the case of a warrant to be issued under section 96(2), the purpose mentioned in section 96(2)(a). 5
- (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 91 or 93, the Secretary of State or a senior official acting on behalf of the Secretary of State; 10
  - (b) in the case of a warrant issued by the Scottish Ministers under section 92, 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 96 by a law enforcement chief or by an appropriate delegate in relation to the law enforcement chief, either – 15
    - (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 is 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. 20
- (6) A warrant that has been cancelled under this section may not be renewed.

*Implementation of warrants* 25

**109 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. 30
- (2) For the purpose of requiring any person to provide assistance in relation to a targeted equipment interference warrant, the implementing authority may – 35
- (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. 40
- (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. 45

- (5) The references in subsections (2) and (3) and sections 110 and 111 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. 5

## 110 Service of warrants outside the United Kingdom

- (1) This section applies to the service of warrants under section 109(2) on a person outside the United Kingdom.
- (2) 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; 10  
15
  - (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 (3)). 20
- (3) A copy of a warrant may be served on a person outside the United Kingdom in the way mentioned in subsection (2)(c) only if –
- (a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (2)(a) or (b) or otherwise), and 25
  - (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. 30
- (4) The steps mentioned in subsection (3)(b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.
- (5) In this section, “implementing authority” has the same meaning as in section 109.

## 111 Duty of telecommunications operators to assist with implementation 35

- (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 91 or 93, or by the Scottish Ministers under section 92, 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. 40
- (2) A telecommunications operator that has been served with a copy of a targeted equipment interference warrant issued under section 96 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. 5
- (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; 10
  - (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 15
  - (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 is not reasonably practicable for the telecommunications operator to take.
- (6) Where obligations have been imposed on a telecommunications operator (“P”) under section 217 (maintenance of technical capability), 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. 20
- (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. 25

*Supplementary provision*

- 112 Safeguards relating to retention and disclosure of material** 30
- (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. 35  
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; 40
    - (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 addressed, 5
  - (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, 10
  - (d) it is necessary for the purpose of legal proceedings, or
  - (e) it is necessary for the performance of the functions of any person by or 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. 15
- (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)). 20
- (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 25
  - (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 91, grounds falling within section 91(5); 30
  - (b) in relation to a warrant issued under section 92, the purpose of preventing or detecting serious crime;
  - (c) in relation to a warrant issued under section 93, the interests of national security; 35
  - (d) in the case of a warrant issued under section 96(1), the purpose mentioned in section 96(1)(a);
  - (e) in the case of a warrant issued under section 96(2), the purpose mentioned in section 96(2)(a).
- (8) Where an item subject to legal privilege is retained following its examination under a warrant issued under this Part, the person retaining it must inform the Investigatory Powers Commissioner as soon as is reasonably practicable. 40
- (9) Subsection (10) applies if –
- (a) any material obtained under the warrant has been handed over to any overseas authorities, or 45
  - (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 113).

(11) In this section –

“copy”, in relation to material obtained under a warrant, means any of the following (whether or not in documentary form) – 5

(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, 10

and “copied” is to be read accordingly;

“the issuing authority” means –

(a) in the case of a warrant issued under section 91 or 93, the Secretary of State;

(b) in the case of a warrant issued under section 92, the Scottish Ministers; 15

(c) in the case of a warrant issued under section 96, 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. 20

### 113 Safeguards relating to disclosure of material or data 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 25

(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 112(2) and (5) (“the relevant requirements”) 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. 30

(3) In this section –

“copy” has the same meaning as in section 112;

“issuing authority” also has the same meaning as in that section;

“overseas authorities” means authorities of a country or territory outside the United Kingdom. 35

### 114 Duty not to make unauthorised disclosures 40

(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 45



- (b) the disclosure is not an excepted disclosure (see section 115).
- (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; 5
  - (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. 10
- (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; 15
  - (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.
- 115 Section 114: meaning of “excepted” disclosure 20**
- (1) For the purposes of section 114, a disclosure made in relation to a warrant is an authorised 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); 25
  - (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; 30
  - (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 109(4)).
- (3) Head 2 is – 35
- (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.
- (4) Head 3 is – 40
- (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
- (5) But a disclosure within Head 3 is not an authorised disclosure if it is made with a view to furthering any 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 10
    - (ii) relates to the number of warrants under this Part to which the operator has given effect or has been involved in giving effect;
  - (b) a disclosure of information that does not relate to any particular warrant under this Part but relates to such warrants in general. 15

#### 116 Offence of making unauthorised disclosure

- (1) A person commits an offence if –
  - (a) the person discloses any matter in breach of section 114(1), and
  - (b) the person knew that the disclosure was in breach of that section. 20
- (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 25
    - (ii) to a fine,or to both;
  - (b) on summary conviction in Scotland –
    - (i) to imprisonment for a term not exceeding 12 months, or 30
    - (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, 35or 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. 40

**117 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 96 unless the law enforcement chief considers that there is a British Islands connection.
- (2) The law enforcement chiefs specified in this subsection are – 5
- (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; 10
  - (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;
  - (g) the Chief Constable of the Ministry for Defence Police; 15
  - (h) 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 20  
“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), 25
  - (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 – 30
    - (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 35
    - (iii) equipment data which forms part of, or is connected with, communications or information falling with sub-paragraph (i) or (ii).
- (5) Except as provided by subsections (1) to (3), a targeted equipment interference warrant may be issued under section 96 whether or not the person who has power to issue the warrant considers that there is a British Islands connection. 40

**118 Part 5: interpretation**

- (1) In this Part – 45  
“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; 5
- “equipment data” has the meaning given by section 89;
- “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 88(9); 10
- “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; 15
- (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; 20
- “targeted examination warrant” has the meaning given by section 88(9).
- (2) See also –
- section 223 (telecommunications definitions), 25
- section 225 (general definitions),
- section 226 (index of defined expressions).

## PART 6

### BULK WARRANTS

#### CHAPTER 1 30

#### BULK INTERCEPTION WARRANTS

##### *Bulk interception warrants*

### 119 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. 35
- (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 120). 40
- (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 – 5
- (a) the interception, in the course of their transmission by means of a telecommunication system, of communications described in the warrant; 10
  - (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. 15
- (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 – 20
    - (i) the interception of communications not described in the warrant, and
    - (ii) conduct for obtaining secondary data from such communications; 25
  - (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. 30
- (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 35
  - “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 40
    - (b) any communication from which secondary data is obtained under the warrant.

## 120 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 – 45
  - (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). 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— 10
- (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. 15
- (6) For the meaning of “systems data” and “identifying data”, see section 225. 20

## 121 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— 25
    - (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), 30
  - (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— 35
    - (i) each of the specified operational purposes (see section 125) 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, 40
  - (e) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 132 and 133 (safeguards relating to disclosure etc.) are in force in relation to the warrant, 45
  - (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 122, 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 225. 5
- (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)). 10
- (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. 15
- (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) The matters to be taken into account in considering whether the conditions in paragraphs (b) and (c) of subsection (1) are met include whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means. 20
- (6) 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. 25
- 122 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. 30
- (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 – 35
- (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, 40
- (d) the likely cost of complying with any such requirement, and
- (e) any other effect of the warrant on the operator.



### **123 Approval of warrants by Judicial Commissioners**

- (1) In deciding whether to approve a decision to issue a warrant under section 121, 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, 5
  - (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 125) is a purpose for which the examination of intercepted content or secondary data obtained under the warrant is or may be necessary, and 10
    - (ii) the examination of intercepted content or secondary data for each such purpose is necessary as mentioned in section 121(1)(d)(ii), and 15
  - (d) any matters taken into account in accordance with section 122.
- (2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.
- (3) Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 121, the Judicial Commissioner must give the Secretary of State written reasons for the refusal. 20
- (4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant under section 121, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant. 25

### **124 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. 30

### **125 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. 35
- (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. 40
- (4) In specifying any operational purposes, it is not sufficient simply to use the descriptions contained in section 121(1)(b) or (2), but the purposes may still be general purposes.

- (5) The warrant may, in particular, specify all of the operational purposes which, at the time the warrant is issued, the person to whom it is addressed considers are operational purposes for which intercepted content or secondary data obtained under bulk interception warrants may be selected for examination.
- (6) 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. 5

*Duration, modification and cancellation of warrants*

**126 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— 10
- (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. 15
- (2) For provision about the renewal of warrants, see section 127.

**127 Renewal of warrants**

- (1) If the renewal conditions are met, a bulk interception warrant may be renewed, at any time before it would otherwise cease to have effect, by an instrument issued by the Secretary of State. 20  
 This is subject to subsection (5).
- (2) The renewal conditions are—
- (a) that the Secretary of State considers that the warrant continues to be necessary— 25
    - (i) in the interests of national security, or
    - (ii) on that ground and on any other grounds falling within section 121(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, 30
  - (c) that the Secretary of State considers that— 35
    - (i) each of the specified operational purposes (see section 125) 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. 40
- (3) 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.

- (4) Section 123 (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.  
This is subject to subsection (5).
- (5) 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 121(1)(b) or (2), and
  - (c) section 123 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 121(1)(b) or (2).

## 128 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 –
    - (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 121(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) Section 123 (approval of warrants by Judicial Commissioners) applies in relation to a decision to make a major modification of a bulk interception warrant as it applies in relation to the decision to issue a bulk interception warrant.

- Section 129 contains provision about the approval of major modifications made in urgent cases.
- (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. 5
- (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 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. 10
- (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. 15  
 This is subject to subsection (11) (urgent cases).
- (11) In a case where the Secretary of State considers that there is an urgent need to make a major modification –
- (a) the instrument making the modification may be signed by a senior official designated by the Secretary of State for that purpose, and 20
  - (b) the instrument must contain a statement that the case is an urgent case in which the Secretary of State has personally and expressly authorised the making of the modification.
- (12) Despite section 119(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. 25
- (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.
- 129 Approval of major modifications made in urgent cases** 30
- (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. 35
- (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. 40
- “The relevant period” means the period ending with the fifth 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. 5
- (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 – 10
    - (i) anything done before that thing could be stopped, or
    - (ii) anything done which it is not reasonably practicable to stop.

### 130 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. 15
- (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 – 20
- (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 125). 25
- (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. 30
- (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. 35

### *Implementation of warrants*

### 131 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. 40

- 
- (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. 5
- (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. 10
- (5) Sections 35 (service of warrants outside the United Kingdom) and 36 (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. 15
- (6) References in this section (and in sections 35 and 36 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 20
  - (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.*
- 132 Safeguards relating to retention and disclosure of material 25**
- (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 134 are met in relation to the intercepted content or secondary data obtained under the warrant. 30
- 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)) – 35
- (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; 40
  - (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 121(2), 45



- (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, 5
  - (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. 10
- (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. 15
- (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)). 20
- (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 121(2), and 25
  - (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 30
  - (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) 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 133). 35
- (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 40
  - (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, 45
- and “copied” is to be read accordingly;
- “overseas authorities” means authorities of a country or territory outside the United Kingdom.

### 133 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 5
  - (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 132(2) and (5) (“the relevant requirements”) 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 10
  - (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. 15
- (3) In subsection (2)(b) “prohibited disclosure” means a disclosure which, if made in the United Kingdom, would breach the prohibition in section 48(1) (see section 136). 20
- (4) In this section—
- “copy” has the same meaning as in section 132;
  - “overseas authorities” means authorities of a country or territory outside the United Kingdom. 25

### 134 Safeguards relating to examination of material

- (1) For the purposes of section 132 the requirements of this section are met in relation to the intercepted content and secondary data obtained under a warrant if— 30
- (a) any selection 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 35
  - (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 125. 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. 40
- (3) The selection conditions referred to in subsection (1)(c) are— 45

- (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; 5
  - (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. 10
- (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 15
  - (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 – 20
- (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), 25
  - (c) since that time, a written authorisation to examine the relevant content using those criteria has been given by a senior officer, and 30
  - (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 – 35
- (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) – 40
- “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; 45
- “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.

### **135 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 – 5
- (a) the selection of the intercepted content for examination meets any of the selection conditions in section 134(3)(a) to (c), and
- (b) either – 10
- (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. 15
- (3) 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 132 (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 20
- (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. 25
- (4) Where an item subject to legal privilege intercepted in accordance with a bulk interception warrant is retained following its examination, the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable. 30
- (For provision about the grounds for retaining material obtained under a warrant, see section 132.)

### **136 Application of other restrictions in relation to warrants**

- (1) Section 48 and Schedule 3 (exclusion of matters from legal proceedings) apply in relation to bulk interception warrants as they apply in relation to targeted interception warrants. 35
- (2) Sections 49 to 51 (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 50(2)(c) to a requirement for disclosure imposed by virtue of section 34(5) were a reference to such a requirement imposed by virtue of section 131(4). 40

#### *Interpretation*

### **137 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 119;
- “secondary data” has the meaning given by section 120, and references to obtaining secondary data from a communication are to be read in accordance with that section; 5
- “senior official” means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty’s Diplomatic Service; 10
- “the specified operational purposes” has the meaning given by section 125(6).
- (2) See also –
- section 223 (telecommunications definitions),
- section 225 (general definitions), 15
- section 226 (index of defined expressions).

## CHAPTER 2

### BULK ACQUISITION WARRANTS

#### *Bulk acquisition warrants*

- 138 Power to issue bulk acquisition warrants** 20
- (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), 25
- (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 – 30
- (i) each of the specified operational purposes (see section 141) 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, 35
- (d) the Secretary of State considers that satisfactory arrangements made for the purposes of section 150 (general safeguards) are in force in relation to the warrant, and
- (e) the decision to issue the warrant has been approved by a Judicial Commissioner. 40
- For the meaning of “head of an intelligence service”, see section 225.
- (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 45

- (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. 5
- (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. 10
- (5) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether the communications data which it is thought necessary to obtain under the warrant could reasonably be obtained by other means. 15
- (6) 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 (7).
- (7) The activities are—
- (a) requiring a telecommunications operator specified in the warrant— 20
- (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 25
- (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, 30
- (c) the disclosure, in any manner described in the warrant, of such data to the person to whom the warrant is addressed or to any person acting on that person's behalf.
- (8) A bulk acquisition warrant also authorises the following conduct (in addition to the conduct described in the warrant)— 35
- (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. 40
- (9) A bulk acquisition warrant may relate to data whether or not in existence at the time of the issuing of the warrant.
- (10) 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. 45



### **139 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)(a) of that section, 5
  - (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 141) is a purpose for which the examination of communications data obtained under the warrant is or may be necessary, and 10
    - (ii) the examination of such data for each such purpose is necessary as mentioned in section 138(1)(c)(ii).
- (2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review. 15
- (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. 20

### **140 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. 25
- (2) Before a bulk acquisition warrant is issued, it must be signed by the Secretary of State.

### **141 Requirements that must be met by warrants**

- (1) A bulk acquisition warrant must contain a provision stating that it is a bulk acquisition warrant. 30
- (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. 35
- (4) In specifying any operational purposes, it is not sufficient simply to use the descriptions contained in section 138(1)(a) or (2), but the purposes may still be general purposes. 40
- (5) The warrant may, in particular, specify all of the operational purposes which, at the time the warrant is issued, the person to whom it is addressed considers are operational purposes for which communications data obtained under bulk acquisition warrants may be selected for examination.

- (6) In this Chapter “the specified operational purposes”, in relation to bulk acquisition warrants, means the operational purposes specified in the warrant in accordance with this section.

*Duration, modification and cancellation of warrants*

- 142 Duration of warrants** 5
- (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. 10
- (2) For provision about the renewal of warrants, see section 143.
- 143 Renewal of warrants**
- (1) If the renewal conditions are met, a bulk acquisition warrant may be renewed, at any time before it would otherwise cease to have effect, by an instrument issued by the Secretary of State. 15  
This is subject to subsection (5).
- (2) The renewal conditions are—
- (a) that the Secretary of State considers that the warrant continues to be necessary— 20
    - (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, 25
  - (c) that the Secretary of State considers that—
    - (i) each of the specified operational purposes (see section 141) is a purpose for which the examination of communications data obtained under the warrant continues to be, or may be, necessary, and 30
    - (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. 35
- (3) 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.
- (4) Section 139 (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. 40  
This is subject to subsection (5).

- (5) 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 one or more activities falling within section 138(7)(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 138(1)(a) or (2), and 5
  - (c) section 139 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)(a) or (2). 10

#### 144 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. 15
- (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 one or more activities falling within section 138(7)(a). 20
- (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 25
  - (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)(a)). 30
- (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. 35
- (6) Section 139 (approval of warrants by Judicial Commissioners) applies in relation to a decision to make a major modification of a bulk acquisition warrant as it applies in relation to the decision to issue a bulk acquisition warrant.  
Section 145 contains provision about the approval of major modifications made in urgent cases. 40
- (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. 45

- 
- (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 communications data obtained under the warrant is or may be necessary, the person must modify the warrant by removing that operational purpose. 5
- (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) (urgent cases).
- (11) In a case where the Secretary of State considers that there is an urgent need to make a major modification – 10
- (a) the instrument making the modification may be signed by a senior official designated by the Secretary of State for that purpose, and
- (b) the instrument must contain a statement that the case is an urgent case in which the Secretary of State has personally and expressly authorised the making of the modification. 15
- (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.
- 145 Approval of major modifications made in urgent cases** 20
- (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. 25
- (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. 30
- “The relevant period” means the period ending with the fifth 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 35
- (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. 40
- (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 – 45
- (i) anything done before that thing could be stopped, or

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

#### 146 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. 5
- (3) The cancellation conditions are –
- (a) that the warrant is no longer necessary in the interests of national security, 10
  - (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 141). 15
- (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 one or more activities falling within section 138(7)(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. 20
- (6) A warrant that has been cancelled under this section may not be renewed.

#### *Implementation of warrants*

- #### 147 Implementation of warrants 25
- (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. 30
- (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. 35
- (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 obtained under the warrant. 40

- (5) References in this section and in sections 148 and 149 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. 5

#### **148 Service of warrants outside the United Kingdom**

- (1) This section applies to the service of bulk acquisition warrants under section 147(3) on a person outside the United Kingdom.
- (2) A copy of a warrant may be served on the person in any of the following ways (as well as by electronic or other means of service) – 10
- (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; 15
  - (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 (3)). 20
- (3) A copy of a warrant may be served on a person in the way mentioned in subsection (2)(c) only if –
- (a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (2)(a) or (b) or otherwise), and 25
  - (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. 30
- (4) The steps mentioned in subsection (3)(b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.
- (5) In this section “the implementing authority” has the same meaning as in section 147.

#### **149 Duty of operators to assist with implementation** 35

- (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. 40  
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 217 (maintenance of technical capability), for the purposes of 45



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. 5

(6) In this section “the implementing authority” has the same meaning as in section 147.

*Restrictions on use or disclosure of data obtained under warrants etc.* 10

## 150 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 15  
(b) that the requirements of section 151 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)) – 20  
(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, 25  
(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), 30  
(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, 35  
(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 40  
(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 45

- 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 there are no longer any relevant grounds for retaining it (see subsection (6)). 5
- (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 138(2), and 10
- (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 15
- (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) 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. 20
- (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) will apply, to such extent (if any) as the Secretary of State considers appropriate, in relation to such data or copy. 25
- (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)— 30
- (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, 35
- and “copied” is to be read accordingly,
- “overseas authorities” means authorities of a country or territory outside the United Kingdom.

### **151 Safeguards relating to examination of data**

- (1) For the purposes of section 150 the requirements of this section are met in relation to the communications data obtained under a warrant if— 40
- (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. 45

- (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 141.
- (3) In subsection (2) “specified in the warrant” means specified in the warrant at the time of the selection of the data for examination. 5

*Supplementary provision*

**152 Offence of making unauthorised disclosure**

- (1) It is an offence for –
- (a) a telecommunications operator who is under a duty by virtue of section 149 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. 15
- (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; 20
  - (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; 25
  - (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; 30
  - (d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both. 35

**153 Chapter 2: interpretation**

- (1) In this Chapter –
- “communications data” does not include communications data within the meaning given by section 224(3),
  - “senior official” means – 40
    - (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 141(6).

- (2) See also –  
 section 223 (telecommunications definitions),  
 section 225 (general definitions), 5  
 section 226 (index of defined expressions).

### CHAPTER 3

#### BULK EQUIPMENT INTERFERENCE WARRANTS

##### *Bulk equipment interference warrants*

- 154 Bulk equipment interference warrants: general** 10
- (1) For the purposes of this Act, a warrant is “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 – 15
    - (i) communications (see section 173);
    - (ii) equipment data (see section 155);
    - (iii) any other information;
  - (c) the main purpose of the warrant is to obtain one or more of the following – 20
    - (i) overseas-related communications;
    - (ii) overseas-related information;
    - (iii) overseas-related equipment data.
- (2) In this Chapter –
- “overseas-related communications” means – 25
    - (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. 30
- (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; 35
  - (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. 40
- (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 2(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.

## 155 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 225.

## 156 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 – 5
- (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 – 10
    - (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, 15
  - (d) the Secretary of State considers that –
    - (i) each of the specified operational purposes (see section 161) is a purpose for which the examination of material obtained under the warrant is or may be necessary, and 20
    - (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 168 and 169 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and 25
  - (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 225. 30
- (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)). 35
- (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. 40
- (4) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether what could be achieved under the warrant could reasonably be achieved by other means.
- (5) 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. 45



### 157 Approval of warrants by Judicial Commissioners

- (1) In deciding whether to approve a decision to issue a warrant under section 156, a Judicial Commissioner must review the Secretary of State’s conclusions on the following matters –
  - (a) whether the warrant is necessary as mentioned in subsection (1)(b) of that section, 5
  - (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 material obtained under the warrant is or may be necessary, and 10
    - (ii) the examination of such material for each such purpose is necessary as mentioned in section 156(1)(d)(ii).
- (2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review. 15
- (3) Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 156, 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 156, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant. 20

### 158 Approval of warrants issued in urgent cases

- (1) This section applies where –
  - (a) a warrant under section 156 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. 25
- (2) The Secretary of State must inform a Judicial Commissioner that it has been issued. 30
- (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. 35“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 (unless already cancelled) ceases to have effect.
- (5) Section 159 contains further provision about what happens if a Judicial Commissioner refuses to approve a decision to issue a warrant. 40

### 159 Failure to approve warrant issued in urgent case

- (1) This section applies where under section 158(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 is addressed to secure that anything in the process of being done under the warrant stops as soon as possible; 5
  - (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. 10
- (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)). 15
- (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. 20
- (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. 25
- (8) Nothing in this section or section 158 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 – 30
    - (i) anything done before that thing could be stopped, or
    - (ii) anything done that it is not reasonably practicable to stop.
- 160 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. 35
- (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. 40
- (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.

### 161 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. 5
- (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. 10
- (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) In specifying any operational purposes, it is not sufficient simply to use the descriptions contained in section 156(1)(b) or (2), but the purposes may still be general purposes. 15
- (6) The warrant may, in particular, specify all of the operational purposes which, at the time the warrant is issued, the person to whom it is addressed considers are operational purposes for which material obtained under bulk equipment interference warrants may be selected for examination. 20
- (7) 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*

### 162 Duration of warrants 25

- (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 163), or
  - (b) it is cancelled or otherwise ceases to have effect before the end of that period (see sections 158 and 166). 30
- (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 – 35
    - (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 – 40
- (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.

### 163 Renewal of warrants

- (1) If the renewal conditions are met, a bulk equipment interference warrant may be renewed, at any time before the end of the relevant period, by an instrument issued by the Secretary of State. 5
- (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 10
- (ii) on that ground and on any other grounds falling within section 156(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, 15
- (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 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 20
- (d) that the decision to renew the warrant has been approved by a Judicial Commissioner. 25
- (3) 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.
- (4) Section 157 (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. 30
- (5) 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 – 35
- (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 156(1)(b) or (2), and
- (c) section 157 has effect as if – 40
- (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 156(1)(b) or (2).

## 164 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 5
  - (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 10
  - (b) any other modification within that subsection is referred to as a “minor modification”. 15
- (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 156(1)(b)). 20
- (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) Section 157 (approval of warrants by Judicial Commissioners) applies in relation to a decision to make a major modification of a bulk equipment interference warrant as it applies in relation to the decision to issue a bulk equipment interference warrant. 25  
Section 165 contains provision about the approval of major modifications made in urgent cases.
- (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. 30
- (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. 35
- (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. 40  
This is subject to subsection (11) (urgent cases).
- (11) In a case where the Secretary of State considers that there is an urgent need to make a major modification –
  - (a) the instrument making the modification may be signed by a senior official designated by the Secretary of State for that purpose, and 45

- (b) the instrument must contain a statement that the case is an urgent case in which the Secretary of State has personally and expressly authorised the making of the modification.
- (12) Despite section 154(1)(a) and (4)(b), 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 regarded as a bulk equipment interference warrant. 5
- (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 by it. 10

### 165 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 15
- (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 – 20
- (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 fifth 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 – 25
- (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. 30
- (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. 35
- (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 – 40
- (i) anything done before that thing could be stopped, or
- (ii) anything done which it is not reasonably practicable to stop.



## 166 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. 5
- (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; 10
  - (c) that the examination of material 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 securing of interference with any equipment or the obtaining of any communications, equipment data or other information. 15
- (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. 20
- (6) A warrant that has been cancelled under this section may not be renewed.

### *Implementation of warrants*

## 167 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. 25 30
- (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. 35
- (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. 40
- (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 110 (service of warrants outside the United Kingdom) and 111 (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 91 by the Secretary of State. 5
- (6) References in this section (and in sections 110 and 111 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 10
  - (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.*

## 168 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 – 15
- (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 170 are met in relation to that material. This is subject to subsection (8). 20
- (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; 25
  - (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 – 30
- (a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 156(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, 35
  - (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 40
  - (e) it is necessary for the performance of the functions of any person by or 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 45

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)). 5
- (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 156(2), and 10
  - (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 15
  - (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) 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 169). 20
- (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) – 25
    - (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; 30
  - “overseas authorities” means authorities of a country or territory outside the United Kingdom.

### 169 Safeguards relating to disclosure of material or data overseas

- (1) The Secretary of State must ensure, in relation to every bulk equipment interference warrant, that arrangements are in force for securing that – 35
- (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 168(2) and (5) (“the relevant requirements”) 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. 40
- (3) In this section – 45

“copy” has the same meaning as in section 168;

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

#### 170 Safeguards relating to examination of material etc.

- (1) For the purposes of section 168, the requirements of this section are met in relation to the material obtained under a warrant if – 5
- (a) any selection of the material obtained under the warrant 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 10
  - (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 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 161. 15
- 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 – 20
- (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; 25
  - (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. 30
- (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 35
  - (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. 40
- (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), 45
  - (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)). 5
- (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. 10
- (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 15
- (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 permitted in subsection (5)(b). 20
- (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 section, “protected material” means any material obtained under the warrant other than material which is – 25
- (a) equipment data;
- (b) information (other than a communication or equipment data) which is not private information.
- 171 Additional safeguards for items subject to legal privilege 30**
- (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 170(3)(a) to (c), and
- (b) either – 35
- (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. 40
- (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) 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 168 (safeguards relating to retention and disclosure of material) 45

- 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
- (4) Where an item subject to legal privilege is retained following its examination under a bulk equipment interference warrant, the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable. 10
- (For provision about the grounds for retaining material obtained under a bulk equipment interference warrant, see section 168.)

## 172 Application of other restrictions in relation to warrants

Sections 114 to 116 (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 115(2)(c) to a requirement for disclosure imposed by virtue of section 109(4) were a reference to such a requirement imposed by virtue of section 167(4). 15

### *Interpretation*

## 173 Chapter 3: interpretation

- (1) In this Chapter – 20
- “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; 25
- “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 155; 30
- “private information” includes information relating to a person’s private or family life;
- “senior official” means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty’s Diplomatic Service; 35
- “the specified operational purposes” has the meaning given by section 161(7).
- (2) See also –
- section 223 (telecommunications definitions);
- section 225 (general definitions); 40
- section 226 (index of defined expressions).



## PART 7

### BULK PERSONAL DATASET WARRANTS

#### *Bulk personal datasets: interpretation*

#### **174 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 section, “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* 20

#### **175 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 176 sets out exceptions to the restrictions imposed by subsections (1) to (3) of this section.

#### **176 Exceptions to section 175(1) and (2)**

- (1) Section 175(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 175(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 189(7) and 190(5) provide for other exceptions to section 175(1) or (2) (in connection with the non-renewal or cancellation of BPD warrants and initial examinations). 5

*Issue of warrants*

**177 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. 10
- (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 wishes to examine bulk personal datasets of that class, the operational purposes for which the intelligence service wishes to do so. 15
- (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 20
    - (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, 25
  - (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 183) is a purpose for which the examination of bulk personal datasets of that class is or may be necessary, and 30
    - (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, 35
  - (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. 40
- (4) 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.

## 178 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 wishes to retain, or to retain and examine, a bulk personal dataset, and 5
  - (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 wishes to retain, or to retain and examine, a bulk personal dataset, and 10
  - (b) the bulk personal dataset falls within a class described in a class BPD warrant but the intelligence service at any time considers that it would be appropriate to seek a specific BPD warrant.
- (4) The application must include – 15
  - (a) a description of the bulk personal dataset to which the application relates, and
  - (b) in a case where the intelligence service wishes to examine the bulk personal dataset, the operational purposes for which the intelligence service wishes to do so. 20
- (5) 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, 25
  - (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, 30
  - (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 183) is a purpose for which the examination of the bulk personal dataset is or may be necessary, and 35
    - (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 40
  - (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.
- (6) 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. 45

- (7) 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.

### 179 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 on the following matters – 5
- (a) whether the warrant is necessary on grounds falling within section 177(3)(a) or (as the case may be) section 178(5)(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 10
  - (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 183) 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 15
    - (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 177(3)(c)(ii) or (as the case may be) section 178(5)(c)(ii). 20
- (2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.
- (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. 25
- (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. 30

### 180 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 believed that there was an urgent need to issue it. 35
- (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. 40
- “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 45

(b) may not be renewed.

- (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 specific BPD warrant issued in urgent case**

- (1) This section applies where under section 180(3) a Judicial Commissioner refuses to approve the decision to issue a warrant. 5
- (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 – 10
- (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 – 15
- (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)). 20
- (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. 25
- (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 – 30
- (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 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 – 35
    - (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 class BPD warrant or a specific BPD warrant must be taken personally by the Secretary of State. 40
- (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
- (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. 10

### 183 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. 15
- (3) A class BPD warrant must –
  - (a) include a description of the class of bulk personal datasets to which the warrant relates, and 20
  - (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, 25
  - (b) where the warrant authorises the retention or examination of replacement datasets, include a description that will enable those datasets to be identified, and
  - (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. 30
- (5) In specifying any operational purposes, it is not sufficient simply to use the descriptions contained in section 177(3)(a) or (as the case may be) section 178(5)(a), but the purposes may still be general ones. 35
- (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, the person to whom it is addressed considers are operational purposes for which data contained in bulk personal datasets of the class described in the warrant, or (as the case may be) data contained in the bulk personal dataset and any replacement datasets described in the warrant, may be selected for examination. 40



*Duration, modification and cancellation*

**184 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 185), or 5
  - (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 180 and 188).
- (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; 10
  - (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. 15
- (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 20
  - (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 185.

**185 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 before the end of the relevant period, by an instrument issued by the Secretary of State. 25
- (2) The renewal conditions are –
  - (a) that the Secretary of State considers that the warrant continues to be necessary on grounds falling within section 177(3)(a) or (as the case may be) section 178(5)(a), 30
  - (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 – 35
    - (i) each of the specified operational purposes (see section 183) 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 40
    - (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 45

- (d) that the decision to renew the warrant has been approved by a Judicial Commissioner.
- (3) 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
- (4) Section 179 (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.

## 186 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. 10
- (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; 15
- (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. 20
- (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”. 25
- (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 177(3)(a) or (as the case may be) section 178(5)(a)). 30
- (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) Section 179 (approval of warrants by Judicial Commissioners) applies in relation to a decision to make a major modification of a class BPD warrant or a specific BPD warrant as it applies in relation to the decision to issue such a warrant. 35
- Section 187 contains provision about the approval of major modifications made in urgent cases. 40
- (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. 45

- (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 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. 5
- (10) 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 (11) (urgent cases).
- (11) In a case where the Secretary of State considers that there is an urgent need to make a major modification – 10
- (a) the instrument making the modification may be signed by a senior official designated by the Secretary of State for that purpose, and
  - (b) the instrument must contain a statement that the case is an urgent case in which the Secretary of State has personally and expressly authorised the making of the modification. 15

#### **187 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 20
  - (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. 25
- (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 fifth working day after the day on which the modification was made. 30
- (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. 35
- (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; 40
  - (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. 45

**188 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. 5
- (3) The cancellation conditions are –
  - (a) that the warrant is no longer necessary on any grounds falling within section 177(3)(a) or (as the case may be) section 178(5)(a); 10
  - (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 183). 15

**189 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. 20
- (2) The head of the intelligence service to whom the warrant is addressed may, before the end of the period of 5 working days beginning with the day on which the warrant ceases to have effect – 25
  - (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; 30
    - (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 35
  - (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. 40
- (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. 45

- (4) 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.
- (5) 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. 5
- (6) 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. 10
- (7) 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 175(1) or (2) by virtue of its retention or examination of any material to which the warrant related during any of the following periods. 15

*First period*

The period of 5 working days beginning with the day on which the warrant ceases to have effect. 20

*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. 25

*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 (6), 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. 30  
35

*Further and supplementary provision*

**190 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 40
- (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. 5
- (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 174). 10
  - 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 the purposes of the exercise of the functions of the intelligence service. 15
  - 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). 20
- (3) The permitted period begins when the head of the intelligence service first forms the beliefs mentioned in subsection (1)(b). 25
- (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. 30
- (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 175(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 35
  - (b) the intelligence service is not to be regarded as in breach of section 175(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. 40

## 191 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— 45



- (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. 5
- (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 183.
- (3) In subsection (2) “specified in the warrant” means specified in the warrant at the time of the selection of the data for examination. 10

## **192 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 175(1) and (2) do not apply by virtue of section 176(1)). 15
- (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 – 20
  - (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 25
  - (c) section 176(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. 30
- (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. 35
- (6) The power conferred by subsection (5) must be exercised to ensure that, where section 48 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). 40
- (7) The Secretary of State may only give a direction under subsection (3) with the approval of a Judicial Commissioner.
- (8) 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. 45

|            |  |           |
|------------|--|-----------|
| (9)        | 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.                           |           |
| (10)       | A direction under subsection (3) –   | 5         |
|            | (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).   |           |
| (11)       | 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 178 (and the Secretary of State may issue such a warrant at the same time as giving the direction). | 10        |
| (12)       | 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 –  | 15        |
|            | (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).   |           |
| <b>193</b> | <b>Interpretation of Part</b>  | <b>20</b> |
| (1)        | In this Part –   |           |
|            | “class BPD warrant” has the meaning given by section 175(3)(a);  |           |
|            | “specific BPD warrant” has the meaning given by section 175(3)(b);   |           |
|            | “senior official” means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty’s Diplomatic Service.   | 25        |
| (2)        | See also –   |           |
|            | section 225 (general definitions),   |           |
|            | section 226 (index of defined expressions).  |           |
|            | <b>PART 8</b>  | <b>30</b> |
|            | OVERSIGHT ARRANGEMENTS   |           |
|            | <b>CHAPTER 1</b>   |           |
|            | INVESTIGATORY POWERS COMMISSIONER AND OTHER JUDICIAL COMMISSIONERS   |           |
|            | <i>The Commissioners</i>   |           |
| <b>194</b> | <b>Investigatory Powers Commissioner and other Judicial Commissioners</b>  | <b>35</b> |
| (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.   | 40        |

- (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) Before appointing any person under subsection (1), the Prime Minister must consult – 5
- (a) the Lord Chief Justice of England and Wales,
  - (b) the Lord President of the Court of Session,
  - (c) the Lord Chief Justice of Northern Ireland,
  - (d) the Scottish Ministers, and 10
  - (e) the First Minister and deputy First Minister in Northern Ireland.
- (4) Before appointing a Judicial Commissioner under subsection (1)(b), the Prime Minister must also consult the Investigatory Powers Commissioner.
- (5) 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 (3)(d). 15
- (6) 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.
- (7) 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. 20
- (8) References in any enactment –
- (a) to a Judicial Commissioner are to be read as including the Investigatory Powers Commissioner, and 25
  - (b) to the Investigatory Powers Commissioner are to be read, so far as necessary for the purposes of subsection (7), as references to the Investigatory Powers Commissioner or any other Judicial Commissioner. 30

## 195 Terms and conditions of appointment

- (1) Subject as follows, each Judicial Commissioner holds and vacates office in accordance with their 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 194(1). 35
- (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. 40
- (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, 5
  - (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), 10
- (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 15
- (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*

- 196 Main oversight functions** 20
- (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, 25
  - (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 – 30
- (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 35
  - (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, 40
  - (b) the giving and operation of notices under section 216 (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.), 45

- (d) 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.),
  - (e) the adequacy of the arrangements by virtue of which the duties imposed by section 55 of that Act are sought to be discharged, 5
  - (f) the exercise of functions by virtue of the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11) (surveillance and covert human intelligence sources),
  - (g) the exercise of functions under Part 3 of the Police Act 1997 (authorisation of action in respect of property), 10
  - (h) 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
  - (i) 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. 15
- (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, 20
  - (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 – 25
    - (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, 30and 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), (g), (h) or (i) above,
  - (e) the exercise of any function where the conduct concerned is – 35
    - (i) conduct authorised by section 38, 40 or 43, or
    - (ii) conduct authorised by section 39 which is not conduct by or on behalf of an intercepting authority (within the meaning given by section 16(1)), or
  - (f) the exercise of any function which is subject to review by the Information Commissioner. 40
- (5) 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, 45
  - (b) the prevention or detection of serious crime, or
  - (c) the economic well-being of the United Kingdom.
- (6) 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. 5
- (7) Subsections (5) and (6) do not apply in relation to the functions of a Judicial Commissioner of—
- (a) deciding whether to approve the issue, modification or renewal of a warrant or authorisation,
  - (b) deciding what may be done with material when a warrant issued for what was considered to be an urgent need is cancelled, or 10
  - (c) reviewing any decision of the kind mentioned in paragraph (a) or (b).
- (8) In this section—
- “bulk personal dataset” is to be read in accordance with section 174,
  - “equipment data” has the same meaning as in Part 5 (see section 89), 15
  - “judicial authority” means a judge, court or tribunal or any person exercising the functions of a judge, court or tribunal,
  - “police force” has the same meaning as in Part 2 (see section 52(1)),
  - “related systems data” has the meaning given by section 13(6),
  - “relevant Minister” means a Minister of the Crown or government department, the Scottish Ministers, the Welsh Ministers or a Northern Ireland department, 20
  - “secondary data” has the same meaning as in Part 2 (see section 14),
  - “statutory function” means any function conferred by virtue of this Act or any other enactment. 25

## 197 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— 30
  - (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 196. 35
- (3) The Prime Minister may give a direction under this section at the request of the Investigatory Powers Commissioner or otherwise. 45
- (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— 40
  - (a) national security,
  - (b) the prevention or detection of serious crime,
  - (c) the economic well-being of the United Kingdom, or 45



- (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.

## 198 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. 10
- (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. 15
- (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. 20 25
- (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). 30 35
- (7) The Investigatory Powers Commissioner may not inform the person to whom it relates of a relevant error except as provided by this section. 40
- (8) A report under section 201(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 45

- (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 5
  - (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”.
- 199 Additional functions under this Part 10**
- (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 15
  - (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. 20
- (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, 25
  - (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. 30
- (4) Subsection (3) does not apply to any advice or information provided under subsection (2) to the Investigatory Powers Tribunal.
- 200 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. 35
- (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”, 40
  - (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)”, 5
- (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 10
- (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) – 15
- (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”, 20
- (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)”, 25
- (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 30
- (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.) – 35
- (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”, 40
- (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”, and 45
- (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) – 50

- (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”, 5
  - (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)”, 10
  - (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 15
  - (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) – 20
- (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”, 25
  - (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 30
  - (e) in the heading of article 6 for “Surveillance Commissioners” substitute “Judicial Commissioners”.

*Reports and investigation and information powers*

- 201 Annual and other reports** 35
- (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), 40
    - (b) information about the results of such use (including its impact),
    - (c) the information on errors required by virtue of section 198(8), 45
    - (d) information about the funding, staffing and other resources of the Judicial Commissioners, and

- (e) 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
- (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. 10
- (6) On receiving a report from the Investigatory Powers Commissioner under subsection (1), the Prime Minister must –
  - (a) publish the report, and 15
  - (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, 25
  - (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. 30
- (8) The Prime Minister must send a copy of every report and statement as laid before Parliament under subsection (6)(b) to –
  - (a) the Scottish Ministers, and
  - (b) the First Minister and the deputy First Minister in Northern Ireland.
- (9) They must lay that copy report and statement before – 35
  - (a) in the case of the Scottish Ministers, the Scottish Parliament, and
  - (b) in the case of the First Minister and the deputy First Minister in Northern Ireland, the Northern Ireland Assembly.
- (10) 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. 40

## 202 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. 45



- (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. 5
- (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. 10
- (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 198(9)) of which it is aware. 15
- (7) In this section “relevant person” means –
- (a) any member of 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, 20
  - (c) any person who is, has been or may become subject to a requirement to provide assistance by virtue of section 34, 36, 109, 111, 131, 147, 149 or 167, or
  - (d) any person to whom a notice is given under section 49 of the Regulation of Investigatory Powers Act 2000. 25

### **203 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 30
  - (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. 35

#### *Supplementary provision*

### **204 Funding, staff and facilities**

- (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.* 40
- (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,*  
*as the Secretary of State considers necessary for the carrying out of the Commissioners’*  
*functions.*

**205 Power to modify functions** 5

- (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 10
  - (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 228(1)(c)) may, in particular, be exercised by modifying any provision made by or under an enactment (including this Act).

**206 Abolition of existing oversight bodies** 15

- (1) The offices of the following are abolished –
  - (a) the Interception of Communications Commissioner,
  - (b) the Intelligence Services Commissioner,
  - (c) the Investigatory Powers Commissioner for Northern Ireland,
  - (d) the Chief Surveillance Commissioner, 20
  - (e) the other Surveillance Commissioners,
  - (f) the Scottish Chief Surveillance Commissioner, and
  - (g) 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), 25
  - (b) sections 59, 59A and 60 of that Act (the Intelligence Services Commissioner),
  - (c) section 61 of that Act (the Investigatory Powers Commissioner for Northern Ireland), 30
  - (d) sections 62 and 63 of that Act and sections 91 and 107 of the Police Act 1997 (the Surveillance Commissioners),
  - (e) section 64 of the Regulation of Investigatory Powers Act 2000 (delegation of Commissioners’ functions), and
  - (f) sections 2(1) to (9), 3 and 4 of the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11) (the Scottish Surveillance Commissioners). 35
- (3) In this section –
  - “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 40
    - (b) the Assistant Surveillance Commissioners appointed under section 3 of that Act,

“the Scottish Chief Surveillance Commissioner” means the Chief Surveillance Commissioner appointed under section 2(1)(a) of that Act.

## CHAPTER 2

### OTHER ARRANGEMENTS

*Codes of practice* 5

#### 207 Codes of practice

Schedule 7 (codes of practice) has effect.

### *Investigatory Powers Tribunal*

#### 208 Right of appeal from Tribunal

- (1) After section 67 of the Regulation of Investigatory Powers Act 2000 insert – 10
- “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”). 15
- (3) This court is whichever of the following courts appears to the Tribunal to be the most appropriate – 20
- (a) the Court of Appeal in England and Wales,
- (b) the Court of Session,
- (c) the Court of Appeal in Northern Ireland.
- (4) 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. 25
- (5) An appeal under this section – 30
- (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.
- (6) The Tribunal or relevant appellate court must not grant leave to appeal unless it considers that – 35
- (a) the appeal would raise an important point of principle or practice, or
- (b) there is another compelling reason for granting leave.
- (7) 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.” 5
- (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). 10
- (3) After section 68(4) of that Act (requirement to give notice of determinations to complainant) insert – 15
- “(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. 20
- (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. 25
- (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). 35
- (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 – 40
- (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) – 45
- (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(4))”, and
- (b) after subsection (4) insert –
- “(4A) A statutory instrument containing regulations under section 67A(4) may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.”

## 209 Functions of Tribunal in relation to this Act

- (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 48 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;”,
- (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 the Investigatory Powers Act 2016 or a warrant under Chapter 2 of Part 6 of that Act (acquisition of communications data);
- (cza) the giving or varying of an authorisation or notice under Part 3 of that Act or 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;”,

- (d) 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 66 of the Investigatory Powers Act 2016”,
- (e) after subsection (7ZA) insert – 5  
“(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)(cza) or (czc).”,
- (f) in subsection (8) (matters that may be challenged before the Tribunal) for paragraphs (a) and (b) substitute – 10  
“(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;”, and
- (g) after subsection (9) insert – 15  
“(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 14 of the Investigatory Powers Act 2016”.
- (2) In section 67(7) of the Act of 2000 (powers of the Tribunal) – 20  
(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;”,
- (b) in paragraph (aa) for “section 23A or 32A” substitute “section 66 of the Investigatory Powers Act 2016 or section 32A of this Act”, and 25  
(c) in paragraph (b) 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,”. 30
- (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) – 35  
(a) in paragraph (e) –  
(i) for “section 11” substitute “section 34, 109, 131, 147 or 167 of the Investigatory Powers Act 2016”, and  
(ii) for “an interception warrant” substitute “a warrant”, 40
- (b) in paragraph (f) for “section 12” substitute “section 217 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; 45  
(ha) every person to whom a retention notice under Part 4 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 5
  - (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”. 10

*Information Commissioner*

**210 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. 15

*Technical Advisory Board*

**211 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. 20
- (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 or technical capability notices under section 217, 25
  - (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, 30
  - (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). 35
- (3) Regulations under this section may also make provision about quorum and the filling of vacancies.



**PART 9**

MISCELLANEOUS AND GENERAL PROVISIONS

**CHAPTER 1**

MISCELLANEOUS

*Combined warrants and authorisations* 5

**212 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*

**213 Payments towards certain compliance costs** 10

- (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. 15
- (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. 20
- (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. 25
- (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 216 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. 30
- (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.* 35

**214 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. 5
- (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 –* 10  
(i) *grant,*  
(ii) *loan,*  
(iii) *guarantee or indemnity,*  
(iv) *investment, or*  
(v) *incurring expenditure for the benefit of the person assisted, and* 15  
(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* 20
- 215 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.” 25
- (3) In section 5 (warrants: general) –  
(a) in subsection (2), omit “, subject to subsection (3) below,” 30  
(b) omit subsection (3),  
(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),”.
- 216 National security notices** 35
- (1) The Secretary of State may give any telecommunications operator in the United Kingdom a notice (a “national security notice”) requiring the operator to take such specified steps as the Secretary of State considers necessary in the interests of national security.
- (2) The Secretary of State may give a national security notice only if the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct. 40

- (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 5
    - (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. 10
- (4) But a national security notice may not require the taking of any steps the main purpose of which is to do something for which a warrant or authorisation is required under this Act.
- (5) 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. 15
- (6) Sections 218 to 220 contain further provision about national security notices.

## 217 Maintenance of technical capability

- (1) The Secretary of State may give a relevant operator a notice (a “technical capability notice”)— 20
- (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. 25
- (2) 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; 30
  - “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. 35
- (3) 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 (see subsection (9)), and 40
  - (b) that it is (and remains) practicable for those relevant operators to comply with those requirements.
- (4) The obligations that may be specified in regulations under this section include, among other things— 45
- (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; 5
- (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.
- (5) Before making any regulations under this section, the Secretary of State must consult the following persons – 10
- (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. 15
- (6) The only steps that may be specified in a technical capability notice given to a person are steps which the Secretary of State considers to be 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. 20
- (7) A technical capability 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) 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). 25
- (9) In this section “relevant authorisation” means –
- (a) any warrant issued under Part 2, 5 or 6, or
- (b) any authorisation or notice given under Part 3.
- (10) Sections 218 to 220 contain further provision about technical capability notices. 30
- 218 Further provision about notices under section 216 or 217**
- (1) In this section “relevant notice” means –
- (a) a national security notice under section 216, or
- (b) a technical capability notice under section 217.
- (2) Before giving a relevant notice to a person, the Secretary of State must consult that person. 35
- (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, 40
- (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. 45

- (4) Where the relevant notice 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
- (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) – 10
- (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. 15
- (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. 20
- (9) A person to whom a relevant notice is given must comply with the notice.
- (10) The duty imposed by subsection (9) is enforceable – 25
- (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. 30
- (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; 35
  - (b) a bulk interception warrant;
  - (c) an authorisation or notice given under Part 3.

## 219 Variation and revocation of notices

- (1) In this section “relevant notice” means – 40
- (a) a national security notice under section 216, or
  - (b) a technical capability notice under section 217.
- (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). 45

- 
- (4) The Secretary of State may vary a national security notice only if 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.
- (5) 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. 5
- (6) Subsections (2) to (4) and (7) of section 218 apply in relation to varying or revoking a relevant notice as they apply in relation to giving a relevant notice.
- (7) Subsections (5) and (6) of section 218 apply to any notice of the variation or revocation of a relevant notice as they apply to a relevant notice. 10
- (8) 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).
- (9) Any reference in this section or section 218(8) to (11) to a notice given under section 216 or 217 includes a reference to such a notice as varied under this section. 15

## **220 Review by the Secretary of State**

- (1) A person who is given a notice under section 216 or 217 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. 20
- (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). 25
- (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) the Investigatory Powers Commissioner. 30
- (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. 35
- (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— 40  
 (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 219, or
  - (b) give a notice under this section to the person confirming its effect.
- (10) Subsections (5) to (8) of section 218 apply in relation to a notice under subsection (9)(b) above as they apply in relation to a notice under section 216 or 217. 5
- (11) Any reference in this section to a notice under section 216 or 217 includes such a notice as varied under section 219, but only so far as the variation is concerned. 10  
But it does not include a notice varied as mentioned in subsection (9)(a) above.

*Wireless telegraphy*

**221 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. 15
- (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 – 20
- (a) constitutes an offence under section 2 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 5 of that Act).”
- (5) Omit subsection (5). 25
- (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** 30

GENERAL

*Review of operation of Act*

**222 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. 35
- (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 – 5
- (a) publish the report prepared under subsection (1), and
  - (b) lay a copy of it before Parliament.

*Interpretation*

**223 Telecommunications definitions**

- (1) The definitions in this section have effect for the purposes of this Act. 10

*Communication*

- (2) “Communication”, in relation to a telecommunications operator, telecommunications service or telecommunication system, includes – 15
- (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 – 20
- (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, 25
  - (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* 30

- (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* 35

- (5) “Communications data”, in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data – 40
- (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 5
  - (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 10
  - (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, 15
- 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 – 20
  - (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 25
  - (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. 30
- (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 35
  - (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 40
  - (b) controls or provides a telecommunication system which is (wholly or partly) –
    - (i) in the United Kingdom, or
    - (ii) controlled from the United Kingdom. 45

- (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. 5
- (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. 10
- (14) “Private telecommunication system” means any telecommunication system which— 15
- (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. 20

## 224 Postal definitions

- (1) The definitions in this section have effect for the purposes of this Act.

*Communication* 25

- (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— 30
- (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, 35
  - (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) 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. 40

*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, 5
  - (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. 10

*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 15
  - (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 20
  - (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. 25
- (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.

**225 General definitions**

- (1) In this Act – 30
  - “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 – 35
    - (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), 40
  - “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), 45

- “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, 5
  - (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, 10
- “enhanced affirmative procedure” is to be read in accordance with section 229,
- “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 – 15
- (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, 20
- “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 194(1)(a) (and the expression is also to be read in accordance with section 194(8)(b)), 25
- “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), 30
  - (b) in relation to Scotland, means –
    - (i) communications between a professional legal adviser and the adviser’s client, or 35
    - (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 40
  - (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 194(1)(a) or (b) (and the expression is therefore to be read in accordance with section 194(8)(a)), 45
- “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, 50



- “modify” includes amend, repeal or revoke (and related expressions are to be read accordingly),
- “person” (other than in Parts 2 and 5) includes an organisation and any association or combination of persons,
- “person holding office under the Crown” includes any servant of the Crown and any member of Her Majesty’s forces, 5
- “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 10
  - (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 15
  - (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, 20
- “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), 25
- “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, 30
- “systems data” has the meaning given by subsection (4),
- “the Technical Advisory Board” means the Board provided for by section 211, 35
- “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, 40
  - (b) data which may be used to identify any event, or
  - (c) data which may be used to identify 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 any event includes – 45
- (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.

## 226 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.

| <i>Expression</i>   | <i>Provision</i>           |
|---|----------------------------|
| Apparatus   | Section 225(1)             |
| Bulk equipment interference warrant   | Section 154(1)             |
| Bulk interception warrant   | Section 119(1)             |
| Civil proceedings   | Section 225(1)             |
| Communication   | Sections 223(2) and 224(2) |
| Communications data   | Sections 223(5) and 224(3) |
| Content of a communication (in relation to a telecommunications operator, telecommunications service or telecommunication system) | Section 223(6)             |
| Crime   | Section 225(1)             |
| Criminal proceedings  | Section 225(1)             |
| Criminal prosecution  | Section 225(1)             |
| Data  | Section 225(1)             |

| <i>Expression</i>  | <i>Provision</i>              |    |
|--|-------------------------------|----|
| Destroy (in relation to electronic data) and related expressions | Section 225(1)                |    |
| Detecting crime or serious crime                                 | Section 225(6)                |    |
| Enactment  | Section 225(1)                | 5  |
| Enhanced affirmative procedure                                   | Section 225(1)                |    |
| Entity   | Section 223(7)                |    |
| Entity data  | Section 223(3)                |    |
| Events data  | Section 223(4)                |    |
| Examination (in relation to material obtained under a warrant)   | Section 225(7)                | 10 |
| Functions  | Section 225(1)                |    |
| GCHQ   | Section 225(1)                |    |
| Head (in relation to an intelligence service)                    | Section 225(1)                |    |
| Her Majesty's forces   | Section 225(1)                | 15 |
| Identifying data   | Section 225(2) and (3)        |    |
| Intelligence service   | Section 225(1)                |    |
| Interception of communication (postal service)                   | Sections 3(7) and 4           |    |
| Interception of communication (telecommunication system)         | Sections 3(1) to (6) and 4(1) |    |
| Interception of communication in the United Kingdom              | Section 3(8)                  | 20 |
| Internet connection record                                       | Section 54(6)                 |    |
| Investigatory Powers Commissioner                                | Section 225(1)                |    |
| Investigatory Powers Tribunal                                    | Section 225(1)                |    |
| Items subject to legal privilege                                 | Section 225(1)                |    |
| Judicial Commissioner  | Section 225(1)                | 25 |
| Judicial Commissioners   | Section 194(6)                |    |
| Lawful authority (in relation to interception of communication)  | Section 5                     |    |
| Legal proceedings  | Section 225(1)                |    |
| Modify (and related expressions)                                 | Section 225(1)                | 30 |
| Person (other than in Parts 2 and 5)                             | Section 225(1)                |    |
| Person holding office under the Crown                            | Section 225(1)                |    |
| Postal data  | Section 224(4)                |    |
| Postal item  | Section 224(5)                |    |
| Postal item in course of transmission by postal service          | Section 3(7)                  | 35 |

| <i>Expression</i>   | <i>Provision</i>         |    |
|---|--------------------------|----|
| Postal operator   | Section 224(6)           |    |
| Postal service  | Section 224(7)           |    |
| Primary legislation   | Section 225(1)           |    |
| Private telecommunication system  | Section 223(14)          | 5  |
| Public authority  | Section 225(1)           |    |
| Public postal service   | Section 224(8)           |    |
| Public telecommunications service   | Section 223(8)           |    |
| Public telecommunication system   | Section 223(9)           |    |
| Serious crime   | Section 225(1)           | 10 |
| Source of journalistic information  | Section 68(7)            |    |
| Specified and specify (in relation to an authorisation, warrant, notice or regulations) | Section 225(1)           |    |
| Subordinate legislation   | Section 225(1)           |    |
| Systems data  | Section 225(4) and (5)   | 15 |
| Technical Advisory Board  | Section 225(1)           |    |
| Telecommunications operator   | Section 223(10)          |    |
| Telecommunications service  | Section 223(11) and (12) |    |
| Telecommunication system  | Section 223(13)          |    |
| Working day   | Section 225(1)           | 20 |

*Supplementary provision***227 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.

## 228 Regulations

5

- (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.

10

- (2) See sections 63(3) and 64(6) for the procedure for a statutory instrument containing regulations under section 62 to which section 63 applies or (as the case may be) regulations under section 64(4) to which section 64(5) applies (enhanced affirmative procedure).

15

- (3) A statutory instrument containing regulations under—

- (a) section 10(4) or 232(2) which amend or repeal any provision of primary legislation,
- (b) section 39(2),
- (c) section 45(4),
- (d) section 74,
- (e) section 80(1),
- (f) section 205,
- (g) section 211,
- (h) section 217,
- (i) section 220(1), or
- (j) paragraph 33 of Schedule 8,

20

may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.

30

- (4) A statutory instrument containing—

- (a) regulations under section 10(4) or 232(2) to which subsection (3) does not apply,
- (b) regulations under section 56(5), or
- (c) regulations under paragraph 2(1)(b) of Schedule 5,

35

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 8(3),
- (b) regulations under section 50(7)(a),
- (c) regulations under section 62 to which section 63 does not apply,
- (d) regulations under section 64(4) to which section 64(5) does not apply,
- (e) regulations under section 115(6)(a), or
- (f) regulations under section 218(7),

40

45

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. 5
- (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). 10
- (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)). 15
- (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) – 20
- (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. 25

## **229 Enhanced affirmative procedure**

- (1) For the purposes of regulations under section 62 to which section 63 applies and regulations under section 64(4) to which section 64(5) applies, the enhanced affirmative procedure is as follows. 30
- (2) Subsection (3) applies if –
- (a) the Secretary of State has consulted under section 63(2) or (as the case may be) 64(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 35
  - (c) the Secretary of State considers it appropriate to proceed with making such regulations.
- (3) The Secretary of State must lay before Parliament – 40
- (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 – 45



- (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. 5
- (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, 10
- 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 – 15
- (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. 20
- (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. 25
- (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. 30

## 230 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* 35
- (b) *any increase attributable to this Act in the sums payable by virtue of any other Act out of money so provided.*

## 231 Transitional, transitory or saving provision

- (1) Schedule 9 (which contains transitional, transitory and saving provision including a general saving for lawful conduct) has effect. 40
- (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.

### **232 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. 5

#### *Final provision*

### **233 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. 10
- (2) Sections 222 to 230, 231(2), 232(2) and (3) and this section come into force on the day on which this Act is passed.
- (3) Sections 194 and 195 come into force at the end of the period of two months beginning with the day on which this Act is passed. 15
- (4) Subject to subsections (5) and (6), this Act extends to England and Wales, Scotland and Northern Ireland.
- (5) An amendment, repeal or revocation of an enactment has the same extent 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 any of the British overseas territories. 20
- (7) This Act may be cited as the Investigatory Powers Act 2016.

## SCHEDULES

### SCHEDULE 1

Section 6

#### MONETARY PENALTY NOTICES

##### PART 1

#### MONETARY PENALTY NOTICES

5

##### *Payment of monetary penalties*

- 1 (1) A monetary penalty imposed by a monetary penalty notice must be paid to the Commissioner within the period specified in the notice.
- (2) The period specified under sub-paragraph (1) must not be less than 28 days beginning with the day after the day on which the notice is served. 10
- (3) *Any sum received by the Commissioner by virtue of a monetary penalty notice must be paid into the Consolidated Fund.*

##### *Contents of monetary penalty notices*

- 2 A monetary penalty notice must, in particular –
  - (a) state the name and address of the person on whom it is to be served, 15
  - (b) provide details of the notice of intent served on that person (see paragraph 4),
  - (c) state whether the Commissioner has received written representations in accordance with that notice of intent,
  - (d) state the grounds on which the Commissioner serves the monetary penalty notice, 20
  - (e) state the grounds on which the Commissioner decided the amount of the monetary penalty imposed by the monetary penalty notice,
  - (f) state the details of how the monetary penalty is to be paid,
  - (g) provide details of the person’s rights of appeal under paragraph 8 in respect of the monetary penalty notice, 25
  - (h) provide details of the Commissioner’s rights of enforcement under paragraph 9 in respect of the monetary penalty notice.

##### *Enforcement obligations*

- 3 (1) The Commissioner may include an enforcement obligation, or enforcement obligations, in a monetary penalty notice if the Commissioner considers that the interception to which the notice relates is continuing. 30
- (2) Each of the following is an enforcement obligation –

- (a) a requirement on the person on whom the notice is served to cease the interception on a specified day or within a specified period;
  - (b) (where appropriate for achieving such a cessation) a requirement on the person to take specified steps within a specified period, or to refrain from taking specified steps after the end of a specified period. 5
- (3) An enforcement obligation may not have effect before the end of the period of 7 days beginning with the day after the day on which the notice is served.
- (4) Where an enforcement obligation is included in a monetary penalty notice under this paragraph, the notice must state what the obligation is and the grounds for including it. 10

*Consultation requirements before service of monetary penalty notices*

- 4 (1) The Commissioner must proceed in accordance with sub-paragraphs (2) to (7) before serving a monetary penalty notice on a person.
- (2) The Commissioner must serve a notice of intent on the person.
- (3) A notice of intent is a notice that the Commissioner proposes to serve a monetary penalty notice on the person. 15
- (4) A notice of intent served on a person must, in particular –
- (a) state the name and address of the person,
  - (b) state the grounds on which the Commissioner proposes to serve the monetary penalty notice, 20
  - (c) provide an indication of the amount of the monetary penalty that the Commissioner proposes to impose and the Commissioner’s grounds for deciding that amount,
  - (d) state whether the monetary penalty notice is to include any enforcement obligation and, if so, what the obligation is and the grounds for including it, 25
  - (e) state the date on which the Commissioner proposes to serve the monetary penalty notice,
  - (f) inform the person that the person may make written representations in relation to the Commissioner’s proposal within a period specified in the notice, and 30
  - (g) inform the person that the person may, within a period specified in the notice, request an oral hearing before the Commissioner in order to make representations of the kind mentioned in sub-paragraph (6)(b). 35
- (5) No period specified as mentioned in sub-paragraph (4)(f) or (g) may be less than 21 days beginning with the day after the day on which the notice is served.
- (6) Where the person has requested an oral hearing within the period specified for the purpose in the notice – 40
- (a) the Commissioner must arrange such a hearing, and
  - (b) the person may make representations at the hearing about –
    - (i) any matter falling within section 6(3)(c), or
    - (ii) any other matter relating to the Commissioner’s proposal which, by virtue of section 48, the person would be unable to raise on an appeal under paragraph 8. 45

- 
- (7) The Commissioner must consider any representations which have been made by the person in accordance with the notice or sub-paragraph (6).
- (8) If the Commissioner decides not to serve a monetary penalty notice on a person as a result of any representations which have been made by the person in accordance with a notice of intent or sub-paragraph (6), the Commissioner must inform the person of that fact. 5
- 5 (1) The Commissioner may not vary a notice of intent except as set out in sub-paragraph (2).
- (2) The Commissioner may vary a notice of intent by extending the period mentioned in paragraph 4(4)(f) or (g). 10
- (3) Sub-paragraph (1) does not prevent the Commissioner from serving a new notice of intent instead of varying such a notice.
- (4) The Commissioner may cancel a notice of intent.
- (5) A variation or cancellation of a notice of intent is effected by serving on the person on whom the notice was served a notice setting out the variation or cancellation. 15
- 6 (1) The Commissioner must not serve a monetary penalty notice on a person in respect of an interception if any notice of intent in respect of that interception was served on the person more than 3 months earlier.
- (2) But the Commissioner may serve a monetary penalty notice on a person where the service of the notice would otherwise be prevented by sub-paragraph (1) if the Commissioner – 20
- (a) considers it reasonable to do so, and
- (b) includes the reasons for doing so in the monetary penalty notice.
- Variation or cancellation of monetary penalty notices* 25
- 7 (1) The Commissioner may vary or cancel a monetary penalty notice.
- (2) But the Commissioner may not vary a monetary penalty notice in a way that is detrimental to the person on whom it was served (whether by increasing the amount of the monetary penalty, by reducing the period specified in the notice as the period within which the penalty must be paid, by imposing a new enforcement obligation or making an existing enforcement obligation effective earlier or otherwise more onerous, or otherwise). 30
- (3) The Commissioner must –
- (a) in the case of a variation which reduces the amount of a monetary penalty, repay any excess already paid in accordance with the notice, and 35
- (b) in the case of a cancellation, repay any amount already paid in accordance with the notice.
- (4) A variation or cancellation of a monetary penalty notice is effected by serving on the person on whom the monetary penalty notice was served a notice setting out the variation or cancellation. 40
- (5) The Commissioner may not serve another monetary penalty notice on a person in respect of an interception if the Commissioner has cancelled a previous notice served on the person in respect of the same interception.

- (6) If the Commissioner refuses a request by a person to vary or cancel a monetary penalty notice which has been served on the person, the Commissioner must inform the person of that fact.

*Appeals in relation to monetary penalty notices*

- 8 (1) A person on whom a monetary penalty notice is served may appeal to the First-tier Tribunal against— 5
- (a) the monetary penalty notice or any provision of it, or
  - (b) any refusal of a request by the person to serve a notice of variation or cancellation in relation to the monetary penalty notice.
- (2) Where there is an appeal under sub-paragraph (1)(a) in relation to a monetary penalty notice or any provision of it, any requirement in the notice or (as the case may be) provision which does not relate to the imposition of an enforcement obligation need not be complied with until the appeal is withdrawn or finally determined. 10
- (3) Sub-paragraphs (4) to (6) apply in relation to an appeal under sub-paragraph (1)(a). 15
- (4) The First-tier Tribunal must allow the appeal or substitute such other monetary penalty notice as could have been served by the Commissioner if the Tribunal considers— 20
- (a) that the notice to which the appeal relates is not in accordance with the law, or
  - (b) to the extent that the notice involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently.
- (5) In any other case, the First-tier Tribunal must dismiss the appeal. 25
- (6) The First-tier Tribunal may review any determination of fact on which the notice was based.
- (7) Sub-paragraphs (8) to (10) apply in relation to an appeal under sub-paragraph (1)(b).
- (8) The First-tier Tribunal must direct the Commissioner to serve, on such terms as the Tribunal considers appropriate, a notice of variation or cancellation in relation to the monetary penalty notice if the Tribunal considers that the monetary penalty notice ought to be varied or cancelled on those terms. 30
- (9) In any other case, the First-tier Tribunal must dismiss the appeal.
- (10) The First-tier Tribunal may review any determination of fact on which the refusal to serve the notice of variation or cancellation was based. 35

*Enforcement of monetary penalty notices*

- 9 (1) This paragraph applies in relation to any penalty payable to the Commissioner by virtue of a monetary penalty notice.
- (2) In England and Wales or Northern Ireland, the penalty is recoverable— 40
- (a) if the county court in England and Wales or a county court in Northern Ireland so orders, as if it were payable under an order of that court, and



- (b) if the High Court so orders, as if it were payable under an order of that court.
- (3) In Scotland, the penalty is recoverable as if it were payable under an extract registered decree arbitral bearing a warrant for execution issued by the sheriff for any sheriffdom in Scotland. 5
- 10 (1) A person on whom a monetary penalty notice containing an enforcement obligation is served must comply with the obligation.
- (2) The duty imposed by sub-paragraph (1) is enforceable by civil proceedings by the Commissioner 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. 10

### Guidance

- 11 (1) The Commissioner must prepare and issue guidance on how the Commissioner proposes to exercise the Commissioner’s functions under section 6 and this Schedule. 15
- (2) The guidance must, in particular, deal with—
- (a) the manner in which the Commissioner is to deal with claims of a description specified in the guidance which may give rise to grounds for serving a monetary penalty notice,
  - (b) the circumstances in which the Commissioner would consider it appropriate to serve a monetary penalty notice, 20
  - (c) how the Commissioner will determine the amount of the penalty, and
  - (d) the circumstances in which the Commissioner would consider it appropriate to impose an enforcement obligation. 25
- (3) The Commissioner may alter or replace the guidance.
- (4) If the guidance is altered or replaced, the Commissioner must issue the altered or replacement guidance.
- (5) The Commissioner must arrange for the publication, in such form and manner as the Commissioner considers appropriate, of any guidance issued under this paragraph. 30

### Interpretation of Part 1

- 12 In this Part of this Schedule—
- “address” means—
- (a) in the case of a registered company, the address of its registered office, 35
  - (b) in the case of a person (other than a registered company) carrying on a business, the address of the person’s principal place of business in the United Kingdom, and
  - (c) in any other case, the person’s last known address; 40
- “the Commissioner” means the Investigatory Powers Commissioner;
- “enforcement obligation” has the meaning given by paragraph 3(2);
- “monetary penalty notice” means a monetary penalty notice under section 6;

“notice” means notice in writing;  
 “notice of intent” has the meaning given by paragraph 4(3);  
 “registered company” means a company registered under the enactments relating to companies for the time being in force in the United Kingdom.

5

## PART 2

## INFORMATION PROVISIONS

*Information notices*

- 13 (1) The Commissioner may by notice (an “information notice”) request any person on whom the Commissioner is considering whether to serve a Part 1 notice of intent or a Part 1 monetary penalty notice to provide such information as the Commissioner reasonably requires for the purpose of deciding whether to serve it. 10
- (2) Where the Commissioner requests that documents be produced, the Commissioner may take copies of, or extracts from, any document so produced. 15
- (3) An information notice must –
- (a) specify or describe the information to be provided,
  - (b) specify the manner in which, and the period within which, the information is to be provided, 20
  - (c) state that the Commissioner considers that the information is information which the Commissioner reasonably requires for the purpose of deciding whether to serve a Part 1 notice of intent or (as the case may be) a Part 1 monetary penalty notice,
  - (d) state the Commissioner’s grounds for this view, and 25
  - (e) provide details of the rights of appeal under paragraph 15 in respect of the information notice.
- (4) For the purposes of sub-paragraph (3)(b) –
- (a) specifying the manner in which the information is to be provided may include specifying the form in which it is to be provided, and 30
  - (b) the specified period within which the information is to be provided must not be less than 28 days beginning with the day after the day on which the information notice is served.
- 14 (1) The Commissioner may not vary an information notice except as set out in sub-paragraph (2). 35
- (2) The Commissioner may vary an information notice by extending the period within which the information is to be provided if the person on whom the notice is served appeals under paragraph 15 in relation to the notice.
- (3) Sub-paragraph (1) does not prevent the Commissioner from serving a new information notice instead of varying such a notice. 40
- (4) The Commissioner may cancel an information notice.
- (5) A variation or cancellation of an information notice is effected by serving on the person on whom the notice was served a notice setting out the variation or cancellation.

*Appeals in relation to information notices*

- 15 (1) A person on whom an information notice is served may appeal to the First-tier Tribunal against –
- (a) the information notice or any provision of it, or
  - (b) any refusal of a request by the person to serve a notice of variation or cancellation in relation to the information notice. 5
- (2) Subject to paragraph 14(2), an appeal under this paragraph does not affect the need to comply with the information notice while the appeal has not been withdrawn or finally determined.
- (3) Sub-paragraphs (4) to (6) apply in relation to an appeal under sub-paragraph (1)(a). 10
- (4) The First-tier Tribunal must allow the appeal or substitute such other information notice as could have been served by the Commissioner if the Tribunal considers –
- (a) that the notice to which the appeal relates is not in accordance with the law, or 15
  - (b) to the extent that the notice involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently.
- (5) In any other case, the First-tier Tribunal must dismiss the appeal. 20
- (6) The First-tier Tribunal may review any determination of fact on which the notice was based.
- (7) Sub-paragraphs (8) to (10) apply in relation to an appeal under sub-paragraph (1)(b).
- (8) The First-tier Tribunal must direct the Commissioner to issue, on such terms as the Tribunal considers appropriate, a notice of variation or cancellation in relation to the information notice if the Tribunal considers that the information notice ought to be varied or cancelled on those terms. 25
- (9) In any other case, the First-tier Tribunal must dismiss the appeal.
- (10) The First-tier Tribunal may review any determination of fact on which the refusal to serve the notice of variation or cancellation was based. 30

*Enforcement of information notices*

- 16 (1) The Commissioner may serve a Part 2 monetary penalty notice on a person if the person –
- (a) without reasonable excuse fails to comply with an information notice, or 35
  - (b) knowingly or recklessly gives any information which is false in a material particular in response to an information notice.
- (2) A Part 2 monetary penalty notice is a notice requiring the person on whom it is served to pay to the Commissioner a monetary penalty of an amount determined by the Commissioner and specified in the notice. 40
- (3) The amount of a monetary penalty determined by the Commissioner under this paragraph may be –
- (a) a fixed amount,

- (b) an amount calculated by reference to a daily rate, or  
(c) a fixed amount and an amount calculated by reference to a daily rate.
- (4) But the total amount payable must not exceed £10,000.
- (5) In the case of an amount calculated by reference to a daily rate –
- (a) no account is to be taken of the day on which the Part 2 monetary penalty notice is served or any day before that day, and 5
- (b) the Part 2 monetary penalty notice must specify –
- (i) the day on which the amount first starts to accumulate and the circumstances in which it is to cease to accumulate, and
- (ii) the period or periods within which the amount, or any part or parts so far accumulated, must be paid to the Commissioner. 10
- Any period falling within paragraph (b)(ii) must not be less than 28 days beginning with the day after the day on which the notice is served.
- 17 (1) *Part 1 of this Schedule applies in relation to a Part 2 monetary penalty notice and the penalty that relates to that notice as it applies in relation to a Part 1 monetary penalty notice and the penalty that relates to that notice.* 15  
This is subject to the following modifications.
- (2) The provisions in Part 1 of this Schedule so far as relating to enforcement obligations do not apply in relation to a Part 2 monetary penalty notice. 20
- (3) Paragraph 4 has effect in relation to a Part 2 monetary penalty notice as if in sub-paragraph (6)(b) the reference to making representations about matters falling within sub-paragraph (6)(b)(i) or (ii) were a reference to making representations about matters falling within sub-paragraph (6)(b)(ii) only.
- (4) Paragraph 6 has effect in relation to a Part 2 monetary penalty notice as if the references in sub-paragraph (1) to an interception were references to conduct falling within paragraph 16(1)(a) or (b). 25
- (5) Paragraph 7(5) has effect in relation to a Part 2 monetary penalty notice as if the references to an interception were references to conduct falling within paragraph 16(1)(a) or (b). 30

*Technical assistance for the Commissioner*

- 18 (1) OFCOM must comply with any reasonable request made by the Commissioner, in connection with the Commissioner’s functions under section 6 and this Schedule, for advice on technical and similar matters relating to electronic communications. 35
- (2) For this purpose, the Commissioner may disclose to OFCOM any information obtained by the Commissioner under this Schedule.
- (3) In this paragraph “OFCOM” means the Office of Communications established by section 1 of the Office of Communications Act 2002.

*Interpretation of Part 2* 40

- 19 In this Part of this Schedule –  
“the Commissioner” means the Investigatory Powers Commissioner;  
“enforcement obligation” has the meaning given by paragraph 3(2);

- “information” includes documents; and any reference to providing or giving information includes a reference to producing a document;
- “information notice” has the meaning given by paragraph 13(1);
- “notice” means notice in writing;
- “Part 1 monetary penalty notice” means a monetary penalty notice under section 6; 5
- “Part 1 notice of intent” means a notice of intent (within the meaning of paragraph 4(3)) relating to a Part 1 monetary penalty notice;
- “Part 2 monetary penalty notice” means a monetary penalty notice under paragraph 16. 10

## SCHEDULE 2

Section 10(1)

### ABOLITION OF DISCLOSURE POWERS

#### *Health and Safety at Work etc. Act 1974*

- 1 In section 20 of the Health and Safety at Work etc. Act 1974 (powers of inspectors), at end, insert – 15
- “(9) Nothing in this section is to be read as enabling an inspector to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.
- (10) In subsection (9) “communications data”, “postal operator” and “telecommunications operator” have the same meanings as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act).” 20

#### *Criminal Justice Act 1987*

- 2 In section 2 of the Criminal Justice Act 1987 (investigation powers of Director of Serious Fraud Office), after subsection (10), insert –
- “(10A) Nothing in this section is to be read as enabling a person to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator. 25
- (10B) In subsection (10A) “communications data”, “postal operator” and “telecommunications operator” have the same meanings as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act).” 30

#### *Consumer Protection Act 1987*

- 3 In section 29 of the Consumer Protection Act 1987 (powers of search etc.), at end, insert –
- “(8) The officer may not exercise a power under this section to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator. 35
- (9) In subsection (8) “communications data”, “postal operator” and “telecommunications operator” have the same meanings as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act).”

*Environmental Protection Act 1990*

- 4 In section 71 of the Environmental Protection Act 1990 (obtaining of information from persons and authorities), at end, insert –
- “(5) Nothing in this section is to be read as enabling a person to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator. 5
- (6) In subsection (5) “communications data”, “postal operator” and “telecommunications operator” have the same meanings as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act).”

*Social Security Administration Act 1992* 10

- 5 In section 109B of the Social Security Administration Act 1992 (power to require information) –
- (a) in subsection (2A) omit paragraph (j),
- (b) in subsection (2E) for the words from “for” to the end of the subsection substitute “so as to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.”, 15
- (c) omit subsection (2F), and
- (d) in subsection (7) –
- (i) after the definition of “bank” insert – 20
- ““communications data” has the same meaning as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act);”,
- (ii) after the definition of “insurer” insert – 25
- ““postal operator” has the same meaning as in the Investigatory Powers Act 2016 (see section 224 of that Act);”, and
- (iii) for the definition of “telecommunications service” substitute – 30
- ““telecommunications operator” has the same meaning as in the Investigatory Powers Act 2016 (see section 223 of that Act).”
- 6 In section 109C of the Social Security Administration Act 1992 (powers of entry) for subsection (6) substitute –
- “(6) Subsections (2E) and (5) of section 109B apply for the purposes of this section as they apply for the purposes of that section.” 35

*Social Security Administration (Northern Ireland) Act 1992*

- 7 In section 103B of the Social Security Administration (Northern Ireland) Act 1992 (power to require information) –
- (a) in subsection (2A) omit paragraph (i), 40
- (b) in subsection (2E) for the words from “for” to the end of the subsection substitute “so as to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.”,
- (c) omit subsection (2F), and 45



- (d) in subsection (7) –
- (i) after the definition of “bank” insert –  
““communications data” has the same meaning as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act);”, 5
  - (ii) after the definition of “insurer” insert –  
““postal operator” has the same meaning as in the Investigatory Powers Act 2016 (see section 224 of that Act);”, and
  - (iii) for the definition of “telecommunications service” substitute – 10  
““telecommunications operator” has the same meaning as in the Investigatory Powers Act 2016 (see section 223 of that Act).”.
- 8 In section 103C of the Social Security Administration (Northern Ireland) Act 1992 (powers of entry) for subsection (6) substitute – 15
- “(6) Subsections (2E) and (5) of section 103B apply for the purposes of this section as they apply for the purposes of that section.”

*Financial Services and Markets Act 2000*

- 9 In section 175 of the Financial Services and Markets Act 2000 (information gathering and investigations: supplemental provision), after subsection (5), insert – 20
- “(5A) Nothing in this Part is to be read as enabling a person to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator. 25
- (5B) In subsection (5A) “communications data”, “postal operator” and “telecommunications operator” have the same meanings as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act).”

*Finance Act 2008*

- 10 In Schedule 36 to the Finance Act 2008 (information and inspection powers), in paragraph 19 (restrictions on powers: types of information), at end, insert – 30
- “(4) An information notice does not require a telecommunications operator or postal operator to provide or produce communications data. 35
- (5) In sub-paragraph (4) “communications data”, “postal operator” and “telecommunications operator” have the same meanings as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act).”

*Prevention of Social Housing Fraud (Power to Require Information) (England) Regulations 2014 (S.I. 2014/899)* 40

- 11 In regulation 4 of the Prevention of Social Housing Fraud (Power to Require Information) (England) Regulations 2014 (power to require information from persons who provide telecommunications services etc.) –

- (a) omit sub-paragraph (f) of paragraph (3),
- (b) in sub-paragraph (g) of that paragraph for “(f)” substitute “(e)”,
- (c) omit paragraphs (6) and (7),
- (d) after paragraph (10) insert –
  - “(10A) Nothing in this regulation is to be read as enabling a person to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.”, and
- (e) in paragraph (11) –
  - (i) after the definition of “bank” insert –
    - ““communications data” has the same meaning as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act);”,
  - (ii) after the definition of “family” insert –
    - ““postal operator” has the same meaning as in the Investigatory Powers Act 2016 (see section 224 of that Act);”, and
  - (iii) for the definition of “telecommunications service” substitute –
    - ““telecommunications operator” has the same meaning as in the Investigatory Powers Act 2016 (see section 223 of that Act).”

## SCHEDULE 3

Section 48

## EXCEPTIONS TO SECTION 48

*Introductory*

- 1 This Schedule contains –
  - (a) exceptions to the exclusion by section 48(1) of certain matters from legal proceedings, and
  - (b) limitations on those exceptions where that exclusion will still apply.

*Disclosures of lawfully intercepted communications*

- 2 (1) Section 48(1)(a) does not prohibit the disclosure of any content of a communication, or any secondary data obtained from a communication, if the interception of that communication was lawful by virtue of any of the following provisions –
  - (a) sections 5(1)(c) and 37 to 45;
  - (b) sections 1(5)(c), 3 and 4 of the Regulation of Investigatory Powers Act 2000;
  - (c) section 1(2)(b) and (3) of the Interception of Communications Act 1985.
- (2) Where any disclosure is proposed to be, or has been, made on the grounds that it is authorised by sub-paragraph (1), section 48(1) does not prohibit the doing of anything in, or for the purposes of, so much of any proceedings as relates to the question whether that disclosure is or was so authorised.

*Disclosures of convictions for certain offences*

- 3 Section 48(1)(b) does not prohibit the doing of anything that discloses any conduct of a person for which that person has been convicted of –
- (a) an offence under section 2(1), 36(7) or 51,
  - (b) an offence under section 1(1) or (2), 11(7) or 19 of the Regulation of Investigatory Powers Act 2000, or 5
  - (c) an offence under section 1 of the Interception of Communications Act 1985.

*Proceedings before the Investigatory Powers Tribunal etc.*

- 4 Section 48(1) does not apply in relation to – 10
- (a) any proceedings before the Investigatory Powers Tribunal,
  - (b) any proceedings on an appeal under section 67A of the Regulation of Investigatory Powers Act 2000 (appeal against decisions of the Tribunal etc.), or
  - (c) any proceedings arising out of such an appeal. 15

*Proceedings before Special Immigration Appeals Commission*

- 5 (1) Section 48(1) does not apply in relation to –
- (a) any proceedings before the Special Immigration Appeals Commission, or
  - (b) any proceedings arising out of proceedings before that Commission. 20
- (2) But sub-paragraph (1) does not permit the disclosure of anything to –
- (a) the appellant or (as the case may be) applicant to the Special Immigration Appeals Commission, or
  - (b) any person who – 25
    - (i) represents that appellant or applicant for the purposes of the proceedings, and
    - (ii) does so otherwise than by virtue of appointment under section 6 of the Special Immigration Appeals Commission Act 1997.

*Proceedings before Proscribed Organisations Appeal Commission* 30

- 6 (1) Section 48(1) does not apply in relation to –
- (a) any proceedings before the Proscribed Organisations Appeal Commission, or
  - (b) any proceedings arising out of proceedings before that Commission.
- (2) But sub-paragraph (1) does not permit the disclosure of anything to any of the following – 35
- (a) the applicant to the Commission;
  - (b) the organisation concerned (if different);
  - (c) any person designated under paragraph 6 of Schedule 3 to the Terrorism Act 2000 to conduct the proceedings on behalf of that organisation; 40
  - (d) any person who –
    - (i) represents that appellant or that organisation for the purposes of the proceedings, and

- (ii) does so otherwise than by virtue of an appointment under paragraph 7 of that Schedule.

*Closed material proceedings*

- 7 (1) Section 48(1) does not apply in relation to any section 6 proceedings within the meaning given by section 14(1) of the Justice and Security Act 2013 (certain civil proceedings in which closed material applications may be made). 5
- (2) But sub-paragraph (1) does not permit a prohibited section 6 disclosure.
- (3) In the case of section 6 proceedings where the only relevant person is the Secretary of State, a “prohibited section 6 disclosure” means a disclosure of anything to – 10
- (a) any person, other than the Secretary of State, who is or was a party to the proceedings, or
  - (b) any person who –
    - (i) represents such a person for the purposes of the proceedings, and 15
    - (ii) does so otherwise than by virtue of appointment as a special advocate.
- (4) In the case of section 6 proceedings where the Secretary of State is not the only relevant person, or is not a relevant person but is a party to the proceedings, a “prohibited section 6 disclosure” means a disclosure of anything to – 20
- (a) any person, other than the relevant person concerned or the Secretary of State, who is or was a party to the proceedings, or
  - (b) any person who – 25
    - (i) represents a person within paragraph (a) for the purposes of the proceedings, and
    - (ii) does so otherwise than by virtue of appointment as a special advocate.
- (5) In this paragraph “relevant person”, in relation to section 6 proceedings, has the meaning given by section 14(1) of the Justice and Security Act 2013. 30

*TPIM proceedings*

- 8 (1) Section 48(1) does not apply in relation to –
- (a) any TPIM proceedings, or
  - (b) any proceedings arising out of any TPIM proceedings. 35
- (2) But sub-paragraph (1) does not permit the disclosure of anything to –
- (a) any person, other than the Secretary of State, who is or was a party to the proceedings, or
  - (b) any person who –
    - (i) represents such a person for the purposes of the proceedings, and 40
    - (ii) does so otherwise than by virtue of appointment as a special advocate under Schedule 4 to the Terrorism Prevention and Investigation Measures Act 2011.

- (3) In this paragraph “TPIM proceedings” has the same meaning as in the Terrorism Prevention and Investigation Measures Act 2011.

*TEO proceedings*

- 9 (1) Section 48(1) does not apply in relation to—
- (a) any TEO proceedings, or 5
  - (b) any proceedings arising out of any TEO proceedings.
- (2) But sub-paragraph (1) does not permit the disclosure of anything to—
- (a) any person, other than the Secretary of State, who is or was a party to the proceedings, or
  - (b) any person who— 10
    - (i) represents such a person for the purposes of the proceedings, and
    - (ii) does so otherwise than by virtue of appointment as a special advocate under Schedule 3 to the Counter-Terrorism and Security Act 2015. 15
- (3) In this paragraph “TEO proceedings” has the meaning given by paragraph 1 of Schedule 3 to the Counter-Terrorism and Security Act 2015 (temporary exclusion orders: proceedings).

*Proceedings relating to freezing of terrorist assets etc.*

- 10 (1) Section 48(1) does not apply in relation to— 20
- (a) any financial restrictions proceedings, or
  - (b) any proceedings arising out of such proceedings.
- (2) In this paragraph “financial restrictions proceedings” has the meaning given by section 65 of the Counter-Terrorism Act 2008.
- 11 Section 48(1) does not apply in relation to any proceedings— 25
- (a) on an appeal under section 26, or an application under section 27, of the Terrorist Asset-Freezing etc. Act 2010 (appeals and reviews by the court), or
  - (b) on a claim arising from any matter to which such an appeal or application relates, 30
- or any proceedings arising out of such proceedings.
- 12 But neither paragraph 10 nor paragraph 11 permits the disclosure of anything to—
- (a) any person, other than the Treasury, who is or was a party to the proceedings, or 35
  - (b) any person who—
    - (i) represents such a person for the purposes of the proceedings, and
    - (ii) does so otherwise than by virtue of appointment as a special advocate. 40

*Proceedings relating to release of prisoners etc. in Northern Ireland*

- 13 (1) Section 48(1) does not apply in relation to—
- (a) any proceedings before—

- (i) the Parole Commissioners for Northern Ireland, or
  - (ii) any Sentence Review Commissioners appointed under section 1 of the Northern Ireland (Sentences) Act 1998, or
  - (b) any proceedings arising out of such proceedings.
- (2) But sub-paragraph (1) does not permit the disclosure of anything to – 5
- (a) any person, other than the Secretary of State, who is or was a party to the proceedings, or
  - (b) any person who –
    - (i) represents such a person for the purposes of the proceedings, and 10
    - (ii) does so otherwise than by virtue of appointment as a special advocate.

*Employment or industrial tribunal proceedings*

- 14 (1) Section 48(1) does not apply in relation to any proceedings before an employment tribunal where the applicant, or the applicant’s representatives, are excluded for all or part of the proceedings pursuant to – 15
- (a) a direction to the tribunal by virtue of section 10(5)(b) or (c) of the Employment Tribunals Act 1996 (exclusion from Crown employment proceedings by direction of Minister in interests of national security), or 20
  - (b) a determination of the tribunal by virtue of section 10(6) of that Act (determination by tribunal in interests of national security).
- (2) Section 48(1) does not apply in relation to any proceedings before an industrial tribunal in Northern Ireland where the applicant, or the applicant’s representatives, are excluded for all or part of the proceedings pursuant to – 25
- (a) a direction to the tribunal by virtue of Article 12(5)(b) or (c) of the Industrial Tribunals (Northern Ireland) Order 1996 (S.I. 1996/1921 (N.I. 18)) (exclusion from Crown employment proceedings by direction of Minister in interests of national security), or 30
  - (b) a determination of the tribunal by virtue of Article 12(6) of that Order (determination by tribunal in interests of national security).
- (3) Section 48(1) does not apply in relation to any proceedings arising out of proceedings within sub-paragraph (1) or (2).
- 15 But paragraph 14 does not permit the disclosure of anything to – 35
- (a) the person who is or was the applicant in the proceedings before the employment or industrial tribunal, or
  - (b) any person who –
    - (i) represents that person for the purposes of any proceedings within paragraph 14, and 40
    - (ii) does so otherwise than by virtue of appointment as a special advocate.

*Proceedings relating to dismissal for certain offences*

- 16 Section 48(1) does not prohibit anything done in, for the purposes of, or in connection with, so much of any legal proceedings as relates to the fairness or unfairness of a dismissal on the following grounds – 45



- (a) any conduct constituting an offence under section 2(1), 36(7) or 51;
- (b) any conduct taking place before the coming into force of this paragraph and constituting –
  - (i) an offence under section 1(1) or (2), 11(7) or 19 of the Regulation of Investigatory Powers Act 2000, or 5
  - (ii) an offence under section 1 of the Interception of Communications Act 1985.

*Proceedings on appeals relating to claims of discrimination in Northern Ireland*

- 17 (1) Section 48(1) does not apply in relation to any proceedings on an appeal under Article 80(2) of the Fair Employment and Treatment (Northern Ireland) Order 1998 (S.I. 1998/3162 (N.I. 21)) where – 10
- (a) the appeal relates to a claim of discrimination in contravention of Part 3 of that Order (employment cases) and to a certificate of the Secretary of State that the act concerned was justified for the purpose of safeguarding national security, and 15
  - (b) a party to the appeal, or the party’s representatives, are excluded for all or part of the proceedings by virtue of section 91(4)(b) of the Northern Ireland Act 1998.
- (2) Section 48(1) does not apply in relation to any proceedings arising out of proceedings within sub-paragraph (1). 20
- 18 But paragraph 17 does not permit the disclosure of anything to –
- (a) any person who is or was excluded from all or part of the proceedings mentioned in paragraph 17(1), or
  - (b) any person who –
    - (i) represents such a person for the purposes of any proceedings within paragraph 17, and 25
    - (ii) does so otherwise than by virtue of appointment as a special advocate.

*Civil proceedings for enforcement of duty to assist with implementation of warrants*

- 19 Section 48(1) does not apply in relation to any civil proceedings under section 36(8) of this Act or section 11(8) of the Regulation of Investigatory Powers Act 2000 (enforcement of duty of operators to assist with implementation of warrants). 30

*Proceedings for certain offences*

- 20 (1) Section 48(1) does not apply in relation to any proceedings for a relevant offence. 35
- (2) “Relevant offence” means –
- (a) an offence under any provision of this Act;
  - (b) an offence under section 1 of the Interception of Communications Act 1985; 40
  - (c) an offence under any provision of the Regulation of Investigatory Powers Act 2000;
  - (d) an offence under section 47 or 48 of the Wireless Telegraphy Act 2006;
  - (e) an offence under section 83 or 84 of the Postal Services Act 2000; 45

- (f) an offence under section 4 of the Official Secrets Act 1989 relating to any such information, document or article as is mentioned in subsection (3)(a) or (c) of that section;
  - (g) an offence under section 1 or 2 of the Official Secrets Act 1911 relating to any sketch, plan, model, article, note, document or information which –
    - (i) incorporates, or relates to, the content of any intercepted communication or any secondary data obtained from a communication, or
    - (ii) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur;
  - (h) an offence of perjury committed in the course of any relevant proceedings;
  - (i) an offence of attempting or conspiring to commit an offence falling within any of paragraphs (a) to (h);
  - (j) an offence under Part 2 of the Serious Crime Act 2007 in relation to an offence falling within any of those paragraphs;
  - (k) an offence of aiding, abetting, counselling or procuring the commission of an offence falling within any of those paragraphs;
  - (l) contempt of court committed in the course of, or in relation to, any relevant proceedings.
- (3) In this paragraph –
- “intercepted communication” and “interception-related conduct” have the same meaning as in section 48;
  - “relevant proceedings” means any proceedings mentioned in paragraphs 4 to 19.

#### *Disclosures to prosecutors and judges*

- 21 (1) Nothing in section 48(1) prohibits –
- (a) a disclosure to a person (“P”) conducting a criminal prosecution that is made for the purpose only of enabling P to determine what is required of P by P’s duty to secure the fairness of the prosecution, or
  - (b) a disclosure to a relevant judge in a case in which the judge has ordered the disclosure to be made to the judge alone.
- (2) A relevant judge may order a disclosure under sub-paragraph (1)(b) only if the judge considers that the exceptional circumstances of the case make the disclosure essential in the interests of justice.
- (3) Where in any criminal proceedings –
- (a) a relevant judge orders a disclosure under sub-paragraph (1)(b), and
  - (b) in consequence of that disclosure, the judge considers that there are exceptional circumstances requiring the judge to make a direction under this sub-paragraph,
- the judge may direct the person conducting the prosecution to make for the purposes of the proceedings any admission of fact which the judge considers essential in the interests of justice.
- (4) But nothing in any direction under sub-paragraph (3) may authorise or require anything to be done in contravention of section 48(1).
- (5) In this paragraph “relevant judge” means –

- (a) any judge of the High Court or of the Crown Court or any Circuit judge,
- (b) any judge of the High Court of Justiciary or any sheriff,
- (c) in relation to proceedings before the Court Martial, the judge advocate for those proceedings, or
- (d) any person holding a judicial office that entitles the person to exercise the jurisdiction of a judge falling within paragraph (a) or (b).

5

*Disclosures to inquiries and inquests*

- 22 (1) Nothing in section 48(1) prohibits –
- (a) a disclosure to the panel of an inquiry held under the Inquiries Act 2005, or
  - (b) a disclosure to a person appointed as legal adviser to such an inquiry, where, in the course of the inquiry, the panel has ordered the disclosure to be made to the panel alone or (as the case may be) to the panel and any person appointed as legal adviser to the inquiry.
- (2) The panel of an inquiry may order a disclosure under sub-paragraph (1) only if it considers that the exceptional circumstances of the case make the disclosure essential to enable the inquiry to fulfil its terms of reference.
- (3) Any reference in this paragraph to a person appointed as legal adviser to an inquiry is a reference to a person appointed as solicitor or counsel to the inquiry.
- 23 (1) Section 48(1) does not apply in relation to any restricted proceedings of an inquiry held under the Inquiries Act 2005.
- (2) Proceedings of an inquiry held under that Act are “restricted proceedings” for the purposes of this paragraph if any restrictions imposed under section 19 of that Act on attendance at the inquiry are in force in relation to the proceedings.
- (3) But sub-paragraph (1) does not permit any disclosure which has not been made in accordance with paragraph 22(1) above.
- 24 (1) Nothing in section 48(1) prohibits –
- (a) a disclosure to a person (the “nominated person”) nominated under paragraph 3(1) of Schedule 10 to the Coroners and Justice Act 2009 (investigation by judge or former judge) to conduct an investigation into a person’s death, or
  - (b) a disclosure to a person appointed as legal adviser to an inquest forming part of an investigation conducted by the nominated person, where, in the course of the investigation, the nominated person has ordered the disclosure to be made to the nominated person alone or (as the case may be) to the nominated person and any person appointed as legal adviser to the inquest.
- (2) The nominated person may order a disclosure under sub-paragraph (1) only if the person considers that the exceptional circumstances of the case make the disclosure essential in the interests of justice.
- (3) Nothing in section 48(1) prohibits a disclosure to any other person conducting an investigation under Part 1 of the Coroners and Justice Act

10

15

20

25

30

35

40

45

2009 into a person's death that there is intercepted material in existence which is, or may be, relevant to the investigation.

- (4) Any reference in this paragraph to a person appointed as legal adviser to an inquest is a reference to a person appointed as solicitor or counsel to the inquest.

5

## SCHEDULE 4

Section 61(1)

## RELEVANT PUBLIC AUTHORITIES AND DESIGNATED SENIOR OFFICERS

## PART 1

## TABLE OF AUTHORITIES AND OFFICERS

## Table

10

| (1)<br>Relevant public authority                               | (2)<br>DSO: minimum office, rank or position | (3)<br>Type of communications data that may be obtained by DSO | (4)<br>Paragraphs of section 53(7) specified for DSO |    |
|--|--|--|--|----|
| Police force maintained under section 2 of the Police Act 1996 | Inspector                                    | Entity data  | (a), (b), (c), (d), (e), (g) and (i)                 | 15 |
|  | Superintendent                               | All  | (a), (b), (c), (d), (e), (g) and (i)                 |    |
| Metropolitan police force                                      | Inspector                                    | Entity data  | (a), (b), (c), (d), (e), (g) and (i)                 | 20 |
|  | Superintendent                               | All  | (a), (b), (c), (d), (e), (g) and (i)                 |    |
| City of London police force                                    | Inspector                                    | Entity data  | (a), (b), (c), (d), (e), (g) and (i)                 | 25 |
|  | Superintendent                               | All  | (a), (b), (c), (d), (e), (g) and (i)                 |    |
| Police Service of Scotland                                     | Inspector                                    | Entity data  | (a), (b), (c), (d), (e), (g) and (i)                 |    |
|  | Superintendent                               | All  | (a), (b), (c), (d), (e), (g) and (i)                 | 30 |
| Police Service of Northern Ireland                             | Inspector                                    | Entity data  | (a), (b), (c), (d), (e), (g) and (i)                 |    |
|  | Superintendent                               | All  | (a), (b), (c), (d), (e), (g) and (i)                 | 35 |
| British Transport Police Force                                 | Inspector                                    | Entity data  | (a), (b), (c), (d), (e), (g) and (i)                 |    |
|  | Superintendent                               | All  | (a), (b), (c), (d), (e), (g) and (i)                 |    |
| Ministry of Defence Police                                     | Inspector                                    | Entity data  | (a), (b), (c) and (g)                                | 40 |
|  | Superintendent                               | All  | (a), (b), (c) and (g)                                |    |

| (1)<br>Relevant public authority | (2)<br>DSO: minimum office, rank or position   | (3)<br>Type of communications data that may be obtained by DSO | (4)<br>Paragraphs of section 53(7) specified for DSO |    |
|----------------------------------|--|--|--|----|
| Royal Navy Police                | Lieutenant Commander   | Entity data  | (a), (b), (c) and (g)                                | 5  |
|                                  | Commander  | All  | (a), (b), (c) and (g)                                |    |
| Royal Military Police            | Major  | Entity data  | (a), (b), (c) and (g)                                | 10 |
|                                  | Lieutenant Colonel   | All  | (a), (b), (c) and (g)                                |    |
| Royal Air Force Police           | Squadron Leader  | Entity data  | (a), (b), (c) and (g)                                |    |
|                                  | Wing Commander   | All  | (a), (b), (c) and (g)                                | 15 |
| Security Service                 | General Duties 4 or any other level 4 officer  | Entity data  | (a), (b) and (c)                                     |    |
|                                  | General Duties 3 or any other level 3 officer  | All  | (a), (b) and (c)                                     | 20 |
| Secret Intelligence Service      | Grade 6  | All  | (a), (b) and (c)                                     |    |
| GCHQ                             | GC8  | All  | (a), (b) and (c)                                     |    |
| Ministry of Defence              | Member of the Senior Civil Service or equivalent   | All  | (a)  |    |
|                                  | Grade 7 in the Fraud Defence Unit  | All  | (b)  | 25 |
| Department of Health             | Grade 7 in the Medicines and Healthcare Products Regulatory Agency   | All  | (b), (d) and (e)                                     |    |
|                                  | Grade 7 in the Anti-Fraud Unit   | All  | (b)  | 30 |
| Home Office                      | Immigration inspector or equivalent with responsibility for investigations or other functions relating to immigration and border security                                | All  | (b)  | 35 |
|                                  | Immigration inspector or equivalent with responsibility for anti-corruption in relation to investigations or other functions relating to immigration and border security | All  | (b)  | 40 |
|                                  | Immigration inspector or equivalent with responsibility for asylum fraud investigations  | All  | (b)  | 45 |
|                                  | Immigration inspector or equivalent with responsibility for security and intelligence in the immigration detention estate  | All  | (b), (d) and (i)                                     | 50 |

| (1)<br><i>Relevant public authority</i>                | (2)<br><i>DSO: minimum office, rank or position</i>  | (3)<br><i>Type of communications data that may be obtained by DSO</i> | (4)<br><i>Paragraphs of section 53(7) specified for DSO</i> |    |
|--|--|---|---|----|
| Ministry of Justice                                    | Manager in the security group of the National Offender Management Service responsible for intelligence   | Entity data   | (b) and (d)   | 5  |
|  | Senior manager in the security group of the National Offender Management Service responsible for intelligence                                    | All   | (b) and (d)   | 10 |
| National Crime Agency                                  | Grade 3  | Entity data   | (b), (g) and (i)  | 15 |
|  | Grade 2  | All   | (b), (g) and (i)  |    |
| Her Majesty's Revenue and Customs                      | Higher officer   | Entity data   | (b) and (f)   |    |
|  | Senior officer   | All   | (b) and (f)   |    |
| Department for Transport                               | Enforcement Officer in Maritime and Coastguard Agency  | Entity data   | (b) and (d)   | 20 |
|  | Head of Enforcement in Maritime and Coastguard Agency  | All   | (b) and (d)   | 25 |
|  | Maritime Operations Commander (grade 7) in the Maritime and Coastguard Agency  | All   | (g)   |    |
|  | Principal Inspector in the Air Accident Investigation Branch, the Marine Accident Investigation Branch or the Rail Accident Investigation Branch | All   | (d)   | 30 |
| Department for Work and Pensions                       | Senior Executive Officer in Fraud and Error Services   | All   | (b)   |    |
|  | Senior Executive Officer in the Child Maintenance Group Central Legal Services   | All   | (b)   | 40 |
| Common Services Agency for the Scottish Health Service | Head of Counter Fraud Services   | All   | (b)   |    |
| Competition and Markets Authority                      | Member of the Senior Civil Service with responsibility for cartels and criminal enforcement  | All   | (b)   | 45 |
| Criminal Cases Review Commission                       | Investigations Adviser   | All   | (h)   |    |
| Department for the Economy in Northern Ireland         | Deputy chief inspector in trading standards services   | All   | (b)   | 50 |
| Department of Justice in Northern Ireland              | Governor 4 in the Northern Ireland Prison Service  | All   | (b), (d) and (i)  |    |
| Financial Conduct Authority                            | Head of department in the Enforcement and Market Oversight Division  | All   | (b) and (j)   | 55 |



| (1)<br>Relevant public authority   | (2)<br>DSO: minimum office, rank or position   | (3)<br>Type of communications data that may be obtained by DSO | (4)<br>Paragraphs of section 53(7) specified for DSO |    |
|--|--|--|--|----|
| A fire and rescue authority under the Fire and Rescue Services Act 2004  | Watch Manager (Control)  | All  | (g)  | 5  |
| Food Standards Agency  | Grade 6  | All  | (b)  |    |
| Food Standards Scotland  | Head of the Scottish Food Crime and Incidents Unit   | All  | (b)  | 10 |
| Gambling Commission  | Senior manager   | All  | (b)  |    |
| Gangmasters and Labour Abuse Authority   | Head of operations   | All  | (b)  |    |
| Health and Safety Executive  | Band 1 inspector   | All  | (b), (d) and (e)                                     |    |
| Independent Police Complaints Commission   | Deputy Chair or Director   | All  | (b) and (i)  | 15 |
| Information Commissioner   | Group Manager  | Entity data  | (b)  |    |
|  | Head of enforcement or an equivalent grade   | All  | (b)  |    |
| National Health Service Business Services Authority  | Senior manager (of pay band 8b) in the Counter Fraud and Security Management Services Division | All  | (b)  | 20 |
| A National Health Service Trust established under section 5 of the National Health Service and Community Care Act 1990 whose functions, as specified in its establishment order, include the provision of emergency ambulance services | Director of Operations or Control and Communications Manager                                   | All  | (b)  | 25 |
|  | Duty Manager of Ambulance Trust Control Rooms  | All  | (g)  | 30 |
| Northern Ireland Ambulance Service Health and Social Care Trust  | Watch Manager (Control)  | All  | (g)  | 35 |
|  | Watch Manager (Control)  | All  | (g)  |    |
| Northern Ireland Fire and Rescue Service Board   | Group Manager (Control)  | All  | (b) and (d)  | 40 |
|  | Watch Manager (Control)  | All  | (g)  |    |
| Northern Ireland Health and Social Care Regional Business Services Organisation  | Assistant Director Counter Fraud and Probity Services  | All  | (b)  |    |
| Office of Communications   | Senior associate   | All  | (b)  | 45 |
| Office of the Police Ombudsman for Northern Ireland  | Senior investigating officer   | All  | (b)  |    |
| Police Investigations and Review Commissioner  | Commissioner or Director of Investigations   | All  | (b) and (i)  | 50 |
| Scottish Ambulance Service Board   | Watch Manager (Control)  | All  | (g)  |    |
| Scottish Criminal Cases Review Commission  | Investigations Adviser   | All  | (h)  |    |

| (1)<br>Relevant public authority                          | (2)<br>DSO: minimum office, rank or position | (3)<br>Type of communications data that may be obtained by DSO | (4)<br>Paragraphs of section 53(7) specified for DSO |   |
|---|--|--|--|---|
| Serious Fraud Office                                      | Grade 6                                      | All  | (b)  | 5 |
| Welsh Ambulance Services<br>National Health Service Trust | Watch Manager (Control)                      | All  | (g)  |   |

## PART 2

### INTERPRETATION OF TABLE

- 1 In the table in Part 1 of this Schedule “entity data” means any communications data which is entity data. 10

## SCHEDULE 5

Section 74(5)

### TRANSFER AND AGENCY ARRANGEMENTS WITH PUBLIC AUTHORITIES: FURTHER PROVISIONS

*Particular safeguards in connection with operation of section 60* 15

- 1 (1) The following provisions apply where the functions of the Secretary of State under section 58 are exercisable by a public authority by virtue of regulations under section 74(1). 10
- (2) The measures adopted or arrangements made by the public authority for the purpose of complying with the requirements of section 60 must be such as are approved by the Secretary of State. 20
- (3) Any report required by section 60(6)(b) or (8) must be made to the Secretary of State as well as to the Investigatory Powers Commissioner.

*Requirement for public authority to provide reports to Secretary of State*

- 2 (1) A public authority, when exercising functions by virtue of regulations under section 74(1), must at least once in each calendar year make a report to the Secretary of State on – 25
- (a) the discharge of the functions, and
- (b) such other matters as the Secretary of State may by regulations require. 30
- (2) Regulations under section 74(1) may, in particular, modify sub-paragraph (1) as it has effect in relation to the calendar year in which the regulations come into force or are revoked.
- (3) The Secretary of State may agree to a report under this paragraph being combined with any other report which the public authority concerned is required to, or may, make to the Secretary of State. 35

*Transfer schemes in connection with transfer of functions*

- 3 (1) The Secretary of State may, in connection with regulations under section 74(1), make a scheme for the transfer of property, rights or liabilities.

- (2) The things that may be transferred under a transfer scheme include—
- (a) property, rights and liabilities which could not otherwise be transferred,
  - (b) property acquired, and rights and liabilities arising, after the making of the scheme. 5
- (3) A transfer scheme may make consequential, supplementary, incidental, transitional, transitory or saving provision and may, in particular—
- (a) create rights, or impose liabilities, in relation to property or rights transferred,
  - (b) make provision about the continuing effect of things done by, on behalf of or in relation to the transferor in respect of anything transferred, 10
  - (c) make provision about the continuation of things (including legal proceedings) in the process of being done by, on behalf of or in relation to the transferor in respect of anything transferred, 15
  - (d) make provision for references to the transferor in an instrument or other document in respect of anything transferred to be treated as references to the transferee,
  - (e) make provision for the shared ownership or use of property,
  - (f) if the TUPE regulations do not apply in relation to the transfer, make provision which is the same or similar. 20
- (4) A transfer scheme may provide—
- (a) for modification by agreement,
  - (b) for modifications to have effect from the date when the original scheme came into effect. 25
- (5) *A transfer scheme may confer a discretion on the Secretary of State to pay compensation to any person whose interests are adversely affected by the scheme.*
- (6) A transfer scheme may be included in regulations under section 74(1) but, if not so included, must be laid before Parliament after being made.
- (7) For the purposes of this paragraph references to rights and liabilities include references to— 30
- (a) rights and liabilities relating to a contract of employment, and
  - (b) rights and liabilities of the Crown relating to the terms of employment of individuals in the civil service.
- (8) Accordingly, a transfer scheme may, in particular, provide— 35
- (a) for—
    - (i) an individual employed in the civil service to become an employee of the transferee, or
    - (ii) an employee of the transferor to become an employee of the transferee or an individual employed in the civil service, 40
  - (b) for—
    - (i) the individual’s terms of employment in the civil service to have effect (subject to any necessary modifications) as the terms of the individual’s contract of employment with the transferee, or 45
    - (ii) (as the case may be) the individual’s contract of employment to have effect (subject to any necessary modifications) as the terms of the individual’s contract of employment with the

- transferee or, where the transferee is the Secretary of State,  
the individual's terms of employment with the civil service,
- (c) for the transfer of rights and liabilities of the Crown or another public authority under or in connection with the individual's terms of employment. 5
- (9) In this paragraph –  
 “civil service” means the civil service of the State,  
 “TUPE regulations” means the Transfer of Undertakings (Protection of Employment) Regulations 2006 (S.I. 2006/246),  
 and references to the transfer of property include the grant of a lease. 10

*Tax in connection with transfer schemes*

- 4 (1) *The Treasury may by regulations make provision varying the way in which a relevant tax has effect in relation to –*
- (a) *anything transferred under a transfer scheme, or*
- (b) *anything done for the purposes of, or in relation to, a transfer under a transfer scheme.* 15
- (2) *The provision which may be made under sub-paragraph (1)(a) includes, in particular, provision for –*
- (a) *a tax provision not to apply, or to apply with modifications, in relation to anything transferred,* 20
- (b) *anything transferred to be treated in a specified way for the purposes of a tax provision,*
- (c) *the Secretary of State to be required or permitted to determine, or specify the method for determining, anything which needs to be determined for the purposes of any tax provision so far as relating to anything transferred.* 25
- (3) *The provision which may be made under sub-paragraph (1)(b) includes, in particular, provision for –*
- (a) *a tax provision not to apply, or to apply with modifications, in relation to anything done for the purposes of, or in relation to, the transfer,*
- (b) *anything done for the purposes of, or in relation to, the transfer to have or not have a specified consequence or be treated in a specified way,* 30
- (c) *the Secretary of State to be required or permitted to determine, or specify the method for determining, anything which needs to be determined for the purposes of any tax provision so far as relating to anything done for the purposes of, or in relation to, the transfer.* 35
- (4) *In this paragraph –*
- “relevant tax” means income tax, corporation tax, capital gains tax, stamp duty, stamp duty reserve tax or stamp duty land tax,  
 “tax provision” means any provision –
- (a) *about a relevant tax, and*
- (b) *made by an enactment,*
- “transfer scheme” means a transfer scheme under paragraph 3,  
 and references to the transfer of property include the grant of a lease. 40

*Supplementary and other general provision*

- 5 The power to make regulations under section 74(1) includes, in particular, power to—
  - (a) modify any enactment about a public authority for the purpose of enabling or otherwise facilitating any function under sections 58 to 60 to be exercisable by the public authority, 5
  - (b) impose requirements or confer other functions on a public authority in connection with functions transferred by the regulations.
  
- 6 The power to make regulations under—
  - (a) section 74, or 10
  - (b) paragraph 4 above,
 including that power as extended (whether by section 228(1) or otherwise) may, in particular, be exercised by modifying any enactment (including this Act).

SCHEDULE 6

Section 96 15

ISSUE OF WARRANTS UNDER SECTION 96 ETC: TABLE

PART 1

TABLE: PART 1

| <i>Law enforcement chiefs</i>  | <i>Appropriate delegates</i>   | <i>Appropriate law enforcement officers</i>  |    |
|--|--|--|----|
| The Chief Constable of a police force maintained under section 2 of the Police Act 1996. | The person who is the appropriate deputy chief constable for the purposes of section 12A(1) of the Police Act 1996.                                  | A member of the police force, a member of a collaborative force or a National Crime Agency officer who is included in a collaboration agreement with the police force. | 20 |
|  | The person holding the rank of assistant chief constable designated to act under section 12A(2) of that Act.   |  | 25 |
|  | If it is not reasonably practicable for either of those persons to act, any other person holding the rank of assistant chief constable in the force. |  | 30 |
|  |  |  | 35 |

| <i>Law enforcement chiefs</i>  | <i>Appropriate delegates</i>   | <i>Appropriate law enforcement officers</i>  |
|--|--|--|
| The Commissioner, or an Assistant Commissioner, of the metropolitan police force.          | A person holding the rank of commander in the metropolitan police force.   | A member of the metropolitan police force, a member of a collaborative force or a National Crime Agency officer who is included in a collaboration agreement with the metropolitan police force.     |
|  |  | 5  |
|  |  | 10   |
| The Commissioner of Police for the City of London.   | The person authorised to act under section 25 of the City of London Police Act 1839 or, if it is not reasonably practicable for that person to act, a person holding the rank of commander in the City of London police force. | A member of the City of London police force, a member of a collaborative force or a National Crime Agency officer who is included in a collaboration agreement with the City of London police force. |
|  |  | 15   |
|  |  | 20   |
| The chief constable of the Police Service of Scotland.                                     | Any deputy chief constable or assistant chief constable of the Police Service of Scotland who is designated for the purpose by the chief constable.  | A constable of the Police Service of Scotland.   |
|  |  | 25   |
| The Chief Constable or a Deputy Chief Constable of the Police Service of Northern Ireland. | A person holding the rank of assistant chief constable in the Police Service of Northern Ireland.  | A member of the Police Service of Northern Ireland.  |
|  |  | 30   |
| The Director General of the National Crime Agency.   | A senior National Crime Agency Officer designated for the purpose by the Director General of the National Crime Agency.  | A National Crime Agency officer or a member of a collaborative police force.   |
|  |  | 35   |
| The Chief Constable of the British Transport Police.                                       | A person holding the rank of deputy or assistant chief constable in the British Transport Police.  | A member of the British Transport Police.  |
|  |  | 40   |
| The Chief Constable of the Ministry of Defence Police.                                     | A person holding the rank of deputy chief constable or assistant chief constable in the Ministry of Defence Police.  | A member of the Ministry of Defence Police.  |
|  |  | 45   |



| <i>Law enforcement chiefs</i>                      | <i>Appropriate delegates</i>   | <i>Appropriate law enforcement officers</i> |    |
|--|--|---|----|
| The Provost Marshal of the Royal Navy Police.      | A person holding the position of deputy Provost Marshal in the Royal Navy Police.      | A member of the Royal Navy Police.          | 5  |
| The Provost Marshal of the Royal Military Police.  | A person holding the position of deputy Provost Marshal in the Royal Military Police.  | A member of the Royal Military Police.      | 10 |
| The Provost Marshal of the Royal Air Force Police. | A person holding the position of deputy Provost Marshal in the Royal Air Force Police. | A member of the Royal Air Force Police.     |    |
| PART 2   |  |   | 15 |

TABLE: PART 2

| <i>Law enforcement chiefs</i>  | <i>Appropriate delegates</i>   | <i>Appropriate law enforcement officers</i> |    |
|--|--|---|----|
| An immigration officer who is a senior official and who is designated for the purpose by the Secretary of State.   | A senior official in the department of the Secretary of State by whom functions relating to immigration are exercisable who is designated for the purpose by the Secretary of State. | An immigration officer.                     | 20 |
| An officer of Revenue and Customs who is a senior official and who is designated for the purpose by the Commissioners for Her Majesty's Revenue and Customs. | An officer of Revenue and Customs who is a senior official and who is designated for the purpose by the Commissioners for Her Majesty's Revenue and Customs.                         | An officer of Revenue and Customs.          | 25 |
|  |  |   | 30 |
| A designated customs official who is a senior official and who is designated for the purpose by the Secretary of State.                                      | A designated customs official who is a senior official and who is designated for the purpose by the Secretary of State.  | A designated customs official.              | 35 |
|  |  |   | 40 |



SCHEDULE 7

Section 207

CODES OF PRACTICE

*Scope of codes*

- 1 (1) The Secretary of State must issue one or more codes of practice about the exercise of functions conferred by virtue of this Act. 5
- (2) Sub-paragraph (1) does not apply in relation to –
  - (a) any functions conferred by virtue of this Act on –
    - (i) the Investigatory Powers Commissioner or any other Judicial Commissioner, 10
    - (ii) the Information Commissioner,
    - (iii) the Investigatory Powers Tribunal,
    - (iv) any other court or tribunal, or
    - (v) the Technical Advisory Board,
  - (b) any function to make subordinate legislation which is conferred by virtue of this Act on the Secretary of State or the Treasury. 15
- (3) A code may, in particular, contain provision about the training of people who may exercise functions in relation to which sub-paragraph (1) applies.
- 2 (1) Each code must include –
  - (a) provision designed to protect the public interest in the confidentiality of sources of journalistic information, and 20
  - (b) provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds items subject to legal privilege or relevant confidential information.
- (2) In this paragraph –

“relevant confidential information” means information which is held in confidence by a member of a profession and consists of –

  - (a) personal records or journalistic material which are (or would be if held in England and Wales) excluded material as defined by section 11 of the Police and Criminal Evidence Act 1984, or 30
  - (b) communications between Members of Parliament and their constituents,

and the references in this paragraph to a member of a profession include references to any person acting in the course of any trade, business, profession or other occupation or for the purposes of any paid or unpaid office. 35
- 3 (1) A code about the exercise of functions conferred by virtue of Part 3 must contain provision about communications data held by public authorities by virtue of that Part.
- (2) Such provision must, in particular, include provision about – 40
  - (a) why, how and where the data is held,
  - (b) who may access the data on behalf of the authority,
  - (c) to whom, and under what conditions, the data may be disclosed,
  - (d) the processing of the data for purposes otherwise than in connection with the purposes for which it was obtained or retained, 45

- (e) the processing of the data together with other data,
- (f) the processes for determining how long the data should be held and for the destruction of the data.

*Procedural requirements*

- |   |   |    |
|---|---|----|
| 4 | (1) Before issuing a code the Secretary of State must –   | 5  |
|   | (a) prepare and publish a draft of the code, and  |    |
|   | (b) consider any representations made about it, and may modify the draft.   |    |
|   | (2) The Secretary of State must, in particular, consult the Investigatory Powers Commissioner and, in the case of a code relating to the exercise of functions conferred by virtue of Part 4, the Information Commissioner. | 10 |
|   | (3) A code comes into force in accordance with regulations made by the Secretary of State.  |    |
|   | (4) A statutory instrument containing such regulations may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.                                    | 15 |
|   | (5) When a draft instrument is laid, the code to which it relates must also be laid.  |    |
|   | (6) No draft instrument may be laid until the consultation required by sub-paragraphs (1) and (2) has taken place.  |    |

*Revision of codes* 20

- |   |   |    |
|---|---|----|
| 5 | (1) The Secretary of State may from time to time revise the whole or part of a code.  |    |
|   | (2) Before issuing any revision of a code the Secretary of State must –   |    |
|   | (a) prepare and publish a draft, and  |    |
|   | (b) consider any representations made about it, and may modify the draft.   | 25 |
|   | (3) The Secretary of State must, in particular, consult the Investigatory Powers Commissioner and, in the case of a code relating to the exercise of functions conferred by virtue of Part 4, the Information Commissioner. |    |
|   | (4) A revision of a code comes into force in accordance with regulations made by the Secretary of State.  | 30 |
|   | (5) A statutory instrument containing such regulations must be laid before Parliament if the regulations have been made without a draft having been laid before, and approved by a resolution of, each House of Parliament. |    |
|   | (6) When an instrument or draft instrument is laid, the revision of a code to which it relates must also be laid.   | 35 |
|   | (7) No instrument or draft instrument may be laid until the consultation required by sub-paragraphs (2) and (3) has taken place.  |    |

*Effect of codes*

- |   |  |    |
|---|--|----|
| 6 | (1) A person must have regard to a code when exercising any functions to which the code relates. | 40 |
|---|--|----|

- (2) A failure on the part of a person to comply with any provision of a code does not of itself make that person liable to criminal or civil proceedings.
- (3) A code is admissible in evidence in any such proceedings.
- (4) A court or tribunal may, in particular, take into account a failure by a person to have regard to a code in determining a question in any such proceedings. 5
- (5) A supervisory authority exercising functions by virtue of this Act may take into account a failure by a person to have regard to a code in determining a question which arises in connection with the exercise of those functions.
- (6) In this paragraph “supervisory authority” means –
  - (a) the Investigatory Powers Commissioner or any other Judicial Commissioner, 10
  - (b) the Information Commissioner, or
  - (c) the Investigatory Powers Tribunal.

## SCHEDULE 8

Section 212

### COMBINATION OF WARRANTS AND AUTHORISATIONS 15

#### PART 1

##### COMBINATIONS WITH TARGETED INTERCEPTION WARRANTS

##### *Warrants that may be issued by 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 warrant that combines a targeted interception warrant which the Secretary of State has power to issue under section 17(1) with one or more of the following –
  - (a) a targeted examination warrant which the Secretary of State has power to issue under section 17(2);
  - (b) a targeted equipment interference warrant which the Secretary of State has power to issue under section 91(1); 25
  - (c) a targeted examination warrant which the Secretary of State has power to issue under section 91(3);
  - (d) a warrant which the Secretary of State has power to issue under section 5 of the Intelligence Services Act 1994 (warrants for entry or interference with property or wireless telegraphy); 30
  - (e) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance);
  - (f) an authorisation under section 32 of that Act (authorisation of intrusive surveillance). 35
- 2 The Secretary of State may, on an application made by or on behalf of the Chief of Defence Intelligence, issue a warrant that combines a targeted interception warrant which the Secretary of State has power to issue under section 17(1) with one or more of the following –
  - (a) a targeted equipment interference warrant which the Secretary of State has power to issue under section 93; 40

- (b) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance);
- (c) an authorisation under section 32 of that Act (authorisation of intrusive surveillance).
- 3 (1) The Secretary of State may, on an application made by or on behalf of a relevant intercepting authority, issue a warrant that combines a targeted interception warrant which the Secretary of State has power to issue under section 17(1) with one or more of the following – 5
- (a) a targeted equipment interference warrant which a law enforcement chief has power to issue under section 96; 10
- (b) an authorisation under section 93 of the Police Act 1997 (authorisations to interfere with property);
- (c) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance);
- (d) an authorisation under section 32 of that Act (authorisation of intrusive surveillance). 15
- (2) For the purposes of sub-paragraph (1), each of the following is a “relevant intercepting authority” –
- (a) the Director General of the National Crime Agency;
- (b) the Commissioner of Police of the Metropolis; 20
- (c) the Chief Constable of the Police Service of Northern Ireland;
- (d) the chief constable of the Police Service of Scotland;
- (e) the Commissioners for Her Majesty’s Revenue and Customs.

*Warrants that may be issued by Scottish Ministers*

- 4 The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a warrant that combines a targeted interception warrant which the Scottish Ministers have power to issue under section 19(1) with one or more of the following – 25
- (a) a targeted examination warrant which the Scottish Ministers have power to issue under section 19(2); 30
- (b) a targeted equipment interference warrant which the Scottish Ministers have power to issue under section 92(1);
- (c) a targeted examination warrant which the Scottish Ministers have power to issue under section 92(2);
- (d) a warrant which the Scottish Ministers have power to issue under section 5 of the Intelligence Services Act 1994 (warrants for entry or interference with property or wireless telegraphy). 35
- 5 The Scottish Ministers may, on an application made by or on behalf of the chief constable of the Police Service of Scotland, issue a warrant that combines a targeted interception warrant which the Scottish Ministers have power to issue under section 19(1) with one or more of the following – 40
- (a) a targeted equipment interference warrant which a law enforcement chief has power to issue under section 96;
- (b) an authorisation under section 93 of the Police Act 1997 (authorisations to interfere with property); 45
- (c) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance);



- (d) an authorisation under section 32 of that Act (authorisation of intrusive surveillance).
- 6 The Scottish Ministers may, on an application made by or on behalf of the chief constable of the Police Service of Scotland, issue a warrant that combines a targeted interception warrant which the Scottish Ministers have power to issue under section 19(1) with one or more of the following— 5
- (a) a targeted equipment interference warrant which a law enforcement chief has power to issue under section 96;
  - (b) an authorisation under section 93 of the Police Act 1997 (authorisations to interfere with property); 10
  - (c) an authorisation under section 6 of the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11) (authorisation of directed surveillance);
  - (d) an authorisation under section 10 of that Act (authorisation of intrusive surveillance). 15
- 7 (1) The Scottish Ministers may, on an application made by or on behalf of a relevant intercepting authority, issue a warrant that combines a targeted interception warrant which the Scottish Ministers have power to issue under section 19(1) with one or more of the following— 20
- (a) a targeted equipment interference warrant which a law enforcement chief has power to issue under section 96;
  - (b) an authorisation under section 93 of the Police Act 1997 (authorisations to interfere with property).
- (2) For the purposes of sub-paragraph (1), each of the following is a “relevant intercepting authority”— 25
- (a) the Director General of the National Crime Agency;
  - (b) the Commissioner of Police of the Metropolis;
  - (c) the Chief Constable of the Police Service of Northern Ireland;
  - (d) the Commissioners for Her Majesty’s Revenue and Customs.

PART 2 30

OTHER COMBINATIONS INVOLVING TARGETED EQUIPMENT INTERFERENCE WARRANTS

*Warrants that may be issued by Secretary of State*

- 8 The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a warrant that combines a targeted equipment interference warrant which the Secretary of State has power to issue under section 91(1) with one or more of the following— 35
- (a) a targeted examination warrant which the Secretary of State has power to issue under section 91(3);
  - (b) a targeted examination warrant which the Secretary of State has power to issue under section 17(2); 40
  - (c) a warrant which the Secretary of State has power to issue under section 5 of the Intelligence Services Act 1994 (warrants for entry or interference with property or wireless telegraphy);
  - (d) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance); 45
  - (e) an authorisation under section 32 of that Act (authorisation of intrusive surveillance).

- 9 The Secretary of State may, on an application made by or on behalf of the Chief of Defence Intelligence, issue a warrant that combines a targeted equipment interference warrant which the Secretary of State has power to issue under section 93 with one or more of the following –
- (a) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance); 5
  - (b) an authorisation under section 32 of that Act (authorisation of intrusive surveillance).

*Warrants that may be issued by Scottish Ministers*

- 10 The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a warrant that combines a targeted equipment interference warrant which the Scottish Ministers have power to issue under section 92(1) with one or more of the following –
- (a) a targeted examination warrant which the Scottish Ministers have power to issue under section 92(2); 10
  - (b) a targeted examination warrant which the Scottish Ministers have power to issue under section 19(2); 15
  - (c) a warrant which the Scottish Ministers have power to issue under section 5 of the Intelligence Services Act 1994 (warrants for entry or interference with property or wireless telegraphy). 20

*Warrants that may be issued by other persons*

- 11 (1) A law enforcement chief may, on an application made by a person who is an appropriate law enforcement officer in relation to the chief, issue a warrant that combines a targeted equipment interference warrant which the law enforcement chief has power to issue under section 96 with one or more of the following –
- (a) an authorisation under section 93 of the Police Act 1997 (authorisations to interfere with property);
  - (b) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance); 30
  - (c) an authorisation under section 32 of that Act (authorisation of intrusive surveillance).
- (2) For the purposes of this paragraph, references to a “law enforcement chief” and an “appropriate law enforcement officer” are to be read in accordance with section 96(4). 35
- 12 (1) A law enforcement chief within sub-paragraph (2) may, on an application made by a person who is an appropriate law enforcement officer in relation to the chief, issue a warrant that combines a targeted equipment interference warrant which the law enforcement chief has power to issue under section 96 with one or more of the following –
- (a) an authorisation under section 93 of the Police Act 1997 (authorisations to interfere with property);
  - (b) an authorisation under section 6 of the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11) (authorisation of directed surveillance); 40
  - (c) an authorisation under section 10 of that Act (authorisation of intrusive surveillance). 45

- (2) The law enforcement chiefs mentioned in sub-paragraph (1) are –
- (a) the chief constable of the Police Service of Scotland, and
  - (b) the Police Investigations and Review Commissioner.
- (3) For the purposes of this paragraph, references to a “law enforcement chief” and an “appropriate law enforcement officer” are to be read in accordance with section 96(4). 5

### PART 3

#### COMBINATIONS INVOLVING TARGETED EXAMINATION WARRANTS ONLY

- 13 The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a warrant that combines – 10
- (a) a targeted examination warrant which the Secretary of State has power to issue under section 17(2), with
  - (b) a targeted examination warrant which the Secretary of State has power to issue under section 91(3).
- 14 The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a warrant that combines – 15
- (a) a targeted examination warrant which the Scottish Ministers have power to issue under section 19(2), with
  - (b) a targeted examination warrant which the Scottish Ministers have power to issue under section 92(2). 20

### PART 4

#### COMBINED WARRANTS: SUPPLEMENTARY PROVISION

##### *Introductory*

- 15 In this Part of this Schedule “combined warrant” means a warrant issued under any of Parts 1 to 3 of this Schedule. 25

##### *General*

- 16 (1) Where Part 1, 2 or 3 of this Schedule provides for a person to have power, on an application made by or on behalf of any person (“the applicant”), to issue a combined warrant that includes any warrant or other authorisation, the person may issue a combined warrant containing that warrant or authorisation, whether or not that person would have power, on an application made by or on behalf of the applicant, to issue that warrant, or to give that authorisation, as a single instrument. 30
- (2) Where Part 1, 2 or 3 of this Schedule provides for a person to have power to apply for a combined warrant, the person may apply for a combined warrant containing any warrant or other authorisation that may be included in it, provided that – 35
- (a) the person could apply for that warrant or authorisation as a single instrument, or
  - (b) the organisation on whose behalf the person is acting, or another person who is a member of staff or an officer of the organisation or who is otherwise acting on its behalf, could apply for that warrant or authorisation as a single instrument. 40

- 
- 17 (1) A combined warrant must be addressed to the person by whom, or on whose behalf, the application for the combined warrant was made.
- (2) Any reference in this Act to the person to whom a warrant is or was addressed is to be read, in the case of a combined warrant containing such a warrant, as a reference to the person to whom the combined warrant is or was addressed. 5
- 18 A combined warrant must contain a provision stating which warrants or other authorisations are included in the combined warrant.
- 19 Any reference in any enactment to a warrant or other authorisation of a particular description issued or given under any enactment includes, in the case of a combined warrant containing a warrant or authorisation of that description, a reference to so much of the combined warrant as consists of such a warrant or authorisation. 10
- This is subject to any provision made by or under the following provisions of this Schedule. 15

*Rules about issue etc. applying separately in relation to each part of a combined warrant*

- 20 (1) The law about the following matters, so far as relating to a warrant or other authorisation that may be included in a combined warrant, applies in relation to so much of a combined warrant as consists of such a warrant or authorisation – 20
- (a) any conditions that must be met before such a warrant or authorisation may be issued or given;
  - (b) the grounds on which such a warrant or authorisation may be issued or given;
  - (c) the conduct that may be authorised by such a warrant or authorisation; 25
  - (d) any requirements as to what must be included in such a warrant or authorisation;
  - (e) any conditions that must be met before such a warrant or authorisation may be renewed and the grounds on which it may be renewed; 30
  - (f) any conditions that must be met before such a warrant or authorisation may be modified;
  - (g) the grounds on which such a warrant or authorisation may be modified and the procedural rules that apply to such a modification; 35
  - (h) the circumstances in which such a warrant or authorisation may or must be cancelled.
- (2) In sub-paragraph (1)(g) “procedural rules”, in relation to the modification of a warrant or other authorisation, means the law about any of the following matters – 40
- (a) the involvement of Judicial Commissioners in decisions;
  - (b) the delegation of decisions;
  - (c) the signing of instruments making a modification;
  - (d) urgent cases.
- (3) Sub-paragraph (1) is subject to paragraphs 21 to 26. 45

*Rules about issue etc. applying in relation to combined warrants*

- 21 (1) A combined warrant under Part 1 of this Schedule addressed to any person may only be issued, renewed or cancelled in accordance with the procedural rules that would apply to the issue, renewal or cancellation of a targeted interception warrant addressed to that person (see Chapter 1 of Part 2 of this Act). 5
- (2) In sub-paragraph (1) “procedural rules”, in relation to a warrant, means the law about any of the following matters –
- (a) the involvement of Judicial Commissioners in decisions;
  - (b) the delegation of decisions; 10
  - (c) the signing of warrants;
  - (d) urgent cases.
- (3) But if a combined warrant under paragraph 1 or 4 includes a warrant which the person issuing the combined warrant has power to issue under section 5 of the Intelligence Services Act 1994 (a “section 5 warrant”), any requirement (arising from sub-paragraph (1) above) for the involvement of Judicial Commissioners in the decision whether to issue or renew the combined warrant does not apply in relation to the part of the combined warrant consisting of the section 5 warrant. 15
- 22 (1) A combined warrant under Part 2 of this Schedule addressed to any person may only be issued, renewed or cancelled in accordance with the procedural rules that would apply to the issue, renewal or cancellation of a targeted equipment interference warrant addressed to that person (see Part 5 of this Act). 20
- (2) In sub-paragraph (1) “procedural rules” has the same meaning as in paragraph 21. 25
- (3) But if a combined warrant under paragraph 8 or 10 includes a warrant which the person issuing the combined warrant has power to issue under section 5 of the Intelligence Services Act 1994 (a “section 5 warrant”), any requirement (arising from sub-paragraph (1) above) for the involvement of Judicial Commissioners in the decision whether to issue or renew the combined warrant does not apply in relation to the part of the combined warrant consisting of the section 5 warrant. 30
- 23 (1) A combined warrant under Part 3 of this Schedule addressed to any person may only be issued, renewed or cancelled in accordance with the procedural rules that would apply to the issue, renewal or cancellation of a targeted examination warrant under section 17(2) addressed to that person (see Chapter 1 of Part 2 of this Act). 35
- (2) In sub-paragraph (1) “procedural rules” has the same meaning as in paragraph 21. 40
- 24 (1) In consequence of paragraphs 21 and 22, the following provisions of the Police Act 1997 do not apply in relation to an authorisation under section 93 of that Act which is included in a combined warrant –
- (a) section 96 (notification of authorisations to Judicial Commissioner);
  - (b) section 97 (authorisations requiring approval); 45
  - (c) section 103(1), (2) and (4) (power to quash or cancel authorisations);
  - (d) section 104 (appeals to Investigatory Powers Commissioner).

- 
- (2) Section 103(6) of that Act applies where a combined warrant containing an authorisation under section 93 of that Act is cancelled as it applies where such an authorisation is cancelled under section 103(4) of that Act.
- 25 In consequence of paragraphs 21 and 22, the following provisions of the Regulation of Investigatory Powers Act 2000 do not apply in relation to an authorisation under section 32 of that Act which is included in a combined warrant – 5
- (a) section 35 (notification of authorisations to Judicial Commissioner);
  - (b) section 36 (approval required for authorisations to take effect);
  - (c) section 37(2) to (4) (power to quash or cancel authorisations); 10
  - (d) section 38 (appeals to Investigatory Powers Commissioner).
- 26 In consequence of paragraphs 21 and 22, the following provisions of the Regulation of Investigatory Powers (Scotland) Act 2000 do not apply in relation to an authorisation under section 10 of that Act which is included in a combined warrant – 15
- (a) section 13 (notification of authorisations to Judicial Commissioner);
  - (b) section 14 (approval required for authorisations to take effect);
  - (c) section 15(1) to (3) (power to quash or cancel authorisations);
  - (d) section 16 (appeals to Investigatory Powers Commissioner).
- Modification of rules as to duration* 20
- 27 (1) Where a combined warrant includes warrants or authorisations which (as single instruments) would cease to have effect at the end of different periods, the combined warrant is to cease to have effect at the end of the shortest of the periods (unless renewed).
- (2) But sub-paragraph (1) does not apply to a combined warrant which – 25
- (a) includes an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance),
  - (b) is addressed to the head of an intelligence service, and
  - (c) is issued with the approval of a Judicial Commissioner. 30
- (3) In such a case, the combined warrant (unless it is renewed) is to cease to have effect at the end of the period of 6 months beginning with the day on which it is issued.
- Special rules about the application of this Act to combined warrants*
- 28 (1) This paragraph applies where under section 22(3) a Judicial Commissioner refuses to approve a decision to issue a combined warrant under Part 1 or 3 of this Schedule. 35
- (2) Section 23 has effect in relation to the combined warrant as if –
- (a) any reference in subsection (3) of that section to a targeted interception warrant or targeted examination warrant were a reference to so much of the combined warrant as consisted of such a warrant, and 40
  - (b) any other reference in that section to a warrant were a reference to the combined warrant.



- (3) Where the combined warrant included a targeted equipment interference warrant or targeted examination warrant which the person who issued the combined warrant has power to issue under Part 5 of this Act, section 99 has effect in relation to the combined warrant as if –
- (a) any reference in subsection (3)(b) or (c) of that section to a targeted equipment interference warrant were a reference to so much of the combined warrant as consisted of such a warrant, 5
  - (b) any reference in subsection (4) of that section to a targeted examination warrant were a reference to so much of the combined warrant as consisted of such a warrant, and 10
  - (c) any other reference in that section to a warrant were a reference to the combined warrant.
- 29 Where under section 98(3) a Judicial Commissioner refuses to approve the decision to issue a combined warrant under Part 2 of this Schedule, section 99 has effect in relation to the combined warrant as if – 15
- (a) any reference in subsection (3)(b) or (c) of that section to a targeted equipment interference warrant were a reference to so much of the combined warrant as consisted of such a warrant,
  - (b) any reference in subsection (4) of that section to a targeted examination warrant were a reference to so much of the combined warrant as consisted of such a warrant, and 20
  - (c) any other reference in that section to a warrant were a reference to the combined warrant.
- 30 (1) This paragraph applies to any provision in Part 2 or 5 of this Act that enables a person to whom a warrant is addressed to require the provision of assistance in giving effect to the warrant. 25
- (2) In the case of a combined warrant containing such a warrant, the provision is to be read as enabling the person to whom the combined warrant is addressed to require the provision of assistance in giving effect to so much of the combined warrant as consists of such a warrant. 30
- (3) Accordingly, any power to serve a copy of a warrant for that purpose includes power, in the case of such a combined warrant, to serve the part of the combined warrant consisting of such a warrant.
- 31 Any reference in section 48 (exclusion of matters from legal proceedings) to the making of an application for a warrant, or the issue of a warrant, under Chapter 1 of Part 2 of this Act includes a reference to – 35
- (a) the making of an application for a combined warrant that includes a warrant under that Chapter, so far as relating to disclosing or suggesting the inclusion of such a warrant, or
  - (b) the inclusion of a warrant under that Chapter in a combined warrant. 40
- 32 (1) The reference in section 50(6) to the provisions of Part 2 of this Act is to be read, in the case of a combined warrant containing a targeted interception warrant or targeted examination warrant which the person who issued the combined warrant has power to issue under that Part, as including a reference to this Schedule. 45
- (2) The reference in section 115(4) to the provisions of Part 5 of this Act is to be read, in the case of a combined warrant containing a targeted equipment interference warrant or targeted examination warrant which the person who

issued the combined warrant has power to issue under that Part, as including a reference to this Schedule.

*Power to make consequential amendments*

- 33 The Secretary of State may by regulations make such provision modifying any provision made by or under an enactment (including this Schedule) as the Secretary of State considers appropriate in consequence of any provision made by this Schedule. 5

SCHEDULE 9

Section 231(1)

TRANSITIONAL, TRANSITORY AND SAVING PROVISION

*Lawful interception of communications* 10

- 1 Any agreement which, immediately before the day on which section 8 comes into force, is designated for the purposes of section 1(4) of the Regulation of Investigatory Powers Act 2000 is to be treated, on and after that day, as designated as an international mutual assistance agreement by regulations under section 8 of this Act. 15

*Authorisations for obtaining communications data*

- 2 The reference to the Gangmasters and Labour Abuse Authority in the table in Part 1 of Schedule 4 is to be read, in relation to any time before the day on which section 8(1) of the Immigration Act 2016 (renaming of Gangmasters Licensing Authority) comes into force, as a reference to the Gangmasters Licensing Authority. 20

*Retention of communications data*

- 3 (1) A retention notice under section 1 of the Data Retention and Investigatory Powers Act 2014 which is in force immediately before the commencement day is to be treated, on or after that day, as a retention notice under section 78 of this Act; and Part 4 of this Act is to be read accordingly but as if section 80(1) to (11) were omitted. 25
- (2) In particular –
- (a) anything which, immediately before the commencement day, is in the process of being done by virtue of, or in relation to, a retention notice under section 1 of the Act of 2014 may be continued as if being done by virtue of, or in relation to, a retention notice under section 78 of this Act, and 30
- (b) anything done by virtue of, or in relation to, a retention notice under section 1 of the Act of 2014 is, if in force or effective immediately before the commencement day, to have effect as if done by virtue of, or in relation to, a retention notice under section 78 of this Act so far as that is required for continuing its effect on or after the commencement day. 35
- (3) Sub-paragraphs (1) and (2) cease to apply, in relation to any retention notice under section 1 of the Act of 2014 – 40

- (a) at the end of the period of six months beginning with the commencement day, or
  - (b) if earlier, on the revocation in full of the notice.
- (4) Section 213 applies in relation to costs incurred in complying with a retention notice under section 1 of the Act of 2014 which has continued in force on or after the commencement day as it applies in relation to costs incurred in complying with retention notices under section 78 of this Act but as if section 213(7) were omitted. 5
- (5) The Secretary of State may revoke (whether wholly or in part) a retention notice under section 1 of the Act of 2014.
- (6) The fact that a retention notice under section 1 of the Act of 2014 has, in relation to a particular description of data and a particular operator (or description of operators), ceased to have effect or been revoked does not prevent the giving of a retention notice under section 78 of this Act in relation to the same description of data and the same operator (or description of operators). 10  
15
- (7) In this paragraph “the commencement day” is the day on which section 1(1) of the Act of 2014 is repealed.
- 4 (1) The repeal of section 1(7) of the Data Retention and Investigatory Powers Act 2014 does not affect the continued operation, during the transitional period mentioned in sub-paragraph (2), of regulations made under section 1(7) of that Act. 20
- (2) The transitional period mentioned in this sub-paragraph is the period of six months beginning with the day on which section 1(7) of the Act of 2014 is repealed.
- (3) In their continued operation by virtue of sub-paragraph (1), the regulations made under section 1(7) of the Act of 2014 have effect subject to such modifications (if any) as may be specified in regulations under section 231(2). 25

*Savings for particular purposes*

- 5 Nothing in this Act affects any power conferred on a postal operator by or under any enactment to open, detain or delay any postal packet (within the meaning given by section 125(1) of the Postal Services Act 2000) or to deliver any such packet to a person other than the person to whom it is addressed. 30
- 6 Nothing in Part 4 of this Act prevents the retention of data for the purposes of, or in connection with, legal proceedings (including proceedings which might arise in the future). 35
- 7 The amendments made to the Regulation of Investigatory Powers Act 2000 by sections 3 to 6 of the Data Retention and Investigatory Powers Act 2014 (and those sections) continue to have effect despite section 8(3) of the Act of 2014 (sunset provision for that Act) until the provisions they amend (and those sections) are repealed by this Act in connection with the coming into force of provisions of this Act. 40

*General saving for lawful conduct*

- 8 Nothing in any of the provisions of this Act by virtue of which conduct of any description is or may be authorised by any warrant, authorisation or 45

notice, or by virtue of which information may be obtained in any manner, is to be read –

- (a) as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act, 5
- (b) as otherwise requiring –
  - (i) the issue, grant or giving of such a warrant, authorisation or notice, or
  - (ii) the taking of any step for or towards obtaining the authority of such a warrant, authorisation or notice, 10
 before any such conduct of that description is engaged in, or
- (c) as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act.

## SCHEDULE 10

Section 232(1)

### MINOR AND CONSEQUENTIAL PROVISION 15

#### PART 1

#### GENERAL AMENDMENTS

##### *Police Act 1997*

- 1 In section 93(1A) of the Police Act 1997 (authorisations to interfere with property etc.) after “this Part” insert “or the Investigatory Powers Act 2016”. 20

##### *Northern Ireland Act 1998*

- 2 In paragraph 9(1) of Schedule 3 to the Northern Ireland Act 1998 (reserved matters) for paragraph (a) substitute –
  - “(a) the subject-matter of Parts 2 and 3 of the Regulation of Investigatory Powers Act 2000, so far as relating to the prevention or detection of crime (within the meaning of that Act) or the prevention of disorder; 25
  - (aa) the subject-matter of the following provisions of the Investigatory Powers Act 2016, so far as relating to the prevention or detection of serious crime (within the meaning of that Act) – 30
    - (i) sections 2 to 8 and Schedule 1,
    - (ii) Part 2, and
    - (iii) Chapter 1 of Part 6;
  - (ab) the subject-matter of section 9, Parts 3 and 4 and Chapter 2 of Part 6 of the Investigatory Powers Act 2016, so far as relating to the prevention or detection of crime (within the meaning of that Act) or the prevention of disorder; 35
  - (ac) the subject-matter of section 10 of, and Schedule 2 to, the Investigatory Powers Act 2016, so far as relating to the prevention or detection of crime (within the meaning of that Act);” 40

*Regulation of Investigatory Powers Act 2000*

- 3 The Regulation of Investigatory Powers Act 2000 is amended as follows.
- 4 In section 27(4)(a) (lawful surveillance etc: conduct to be dealt with under other enactments) after “Act” insert “or the Investigatory Powers Act 2016”.
- 5 (1) Section 71 (issue and revision of codes of practice) is amended as follows. 5
- (2) In subsection (2)(a), for “Parts I to III” substitute “Parts 2 and 3”.
- (3) Omit subsection (2A).
- (4) In subsection (8) for “(2A)” substitute “(3)”.
- 6 (1) Section 81(1) (general definitions) is amended as follows.
- (2) For the definition of “apparatus” substitute – 10
- ““apparatus” has the same meaning as in the Investigatory Powers Act 2016 (see section 225(1) of that Act);”.
- (3) For the definition of “communication” substitute –
- ““communication” has the same meaning as in the Investigatory Powers Act 2016 (see sections 223(2) and 224(2) of that Act);”.
- 15
- (4) In the definition of “interception” and cognate expressions, for “section 2” substitute “sections 3 and 4 of the Investigatory Powers Act 2016”.
- (5) For the definitions of “postal service” and “public postal service” substitute – 20
- ““postal service” has the same meaning as in the Investigatory Powers Act 2016 (see section 224(7) of that Act);”.
- (6) Omit the definitions of “private telecommunication system”, “public telecommunications service” and “public telecommunication system”.
- (7) In the definitions of “telecommunication system” and “telecommunications service”, for “the meanings given by section 2(1)” substitute “the same meanings as in the Investigatory Powers Act 2016 (see section 223(11) to (13) of that Act)”. 25

*Political Parties, Elections and Referendums Act 2000*

- 7 In paragraph 28(4) of Schedule 19C to the Political Parties, Elections and Referendums Act 2000 (civil sanctions: disclosure of information) for paragraph (b) substitute – 30
- “(b) any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.”

*Public Finance and Accountability (Scotland) Act 2000 (2000 asp 1)* 35

- 8 (1) The Public Finance and Accountability (Scotland) Act 2000 is amended as follows.
- (2) In section 26B(3) (voluntary disclosure of data to Audit Scotland) for paragraph (b) substitute –
- “(b) which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016,”.
- 40

|  |   |    |
|--|---|----|
| (3)  | In section 26C(3) (power to require disclosure of data) for paragraph (b) substitute—<br>“(b) the disclosure is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.”   |    |
| <i>Social Security Fraud Act 2001</i>                    |   | 5  |
| 9  | In section 4(1)(b) of the Social Security Fraud Act 2001 (arrangements for payments in relation to persons providing a telecommunications service etc.) for “the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “the Investigatory Powers Act 2016”.   |    |
| <i>Social Security Fraud Act (Northern Ireland) 2001</i> |   | 10 |
| 10   | In section 4(1)(b) of the Social Security Fraud Act (Northern Ireland) 2001 (arrangements for payments in relation to persons providing a telecommunications service etc.) for “the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “the Investigatory Powers Act 2016”.  |    |
| <i>Justice (Northern Ireland) Act 2002</i>               |   | 15 |
| 11   | In section 5A(3)(b) of the Justice (Northern Ireland) Act 2002 (disclosure of information to the Northern Ireland Judicial Appointments Commission) for “Part 1 of the Regulation of Investigatory Powers Act 2000” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.   |    |
| <i>Proceeds of Crime Act 2002</i>                        |   | 20 |
| 12   | (1) The Proceeds of Crime Act 2002 is amended as follows.<br>(2) In section 436(3)(b) (disclosure of information to certain Directors) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.<br>(3) In section 438(8)(b) (disclosure of information by certain Directors) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.<br>(4) In section 439(3)(b) (disclosure of information to Lord Advocate and to Scottish Ministers) for “Part 1 of the Regulation of Investigatory Powers Act 2000” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.<br>(5) In section 441(7)(b) (disclosure of information by Lord Advocate and by Scottish Ministers) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. |    |
| <i>Police Reform Act 2002</i>                            |   | 35 |
| 13   | In paragraph 19ZA(2)(c) of Schedule 3 to the Police Reform Act 2002 (handling of complaints and conduct matters etc: power to serve information notice) for “Part 1 of the Regulation of Investigatory Powers Act 2000” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.   |    |
|  |   | 40 |



*Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426)*

- 14 After regulation 5A(8) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (personal data breach) insert –
- “(9) This regulation does not apply in relation to any personal data breach which is to be notified to the Investigatory Powers Commissioner in accordance with a code of practice made under the Investigatory Powers Act 2016.” 5

*Audit and Accountability (Northern Ireland) Order 2003 (S.I. 2003/418 (N.I. 5))*

- 15 In Article 4C(3)(b) of the Audit and Accountability (Northern Ireland) Order 2003 (voluntary provision of data) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. 10

*Public Audit (Wales) Act 2004*

- 16 In section 64C(3)(b) of the Public Audit (Wales) Act 2004 (voluntary provision of data) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. 15

*Constitutional Reform Act 2005*

- 17 In section 107(3)(b) of the Constitutional Reform Act 2005 (disclosure of information to the Judicial Appointments Commission) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. 20

*Commissioners for Revenue and Customs Act 2005*

- 18 In section 22(b) of the Commissioners for Revenue and Customs Act 2005 (data protection, etc) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. 25

*Serious Crime Act 2007*

- 19 (1) The Serious Crime Act 2007 is amended as follows.
- (2) In section 68(4)(b) (disclosure of information to prevent fraud) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. 30
- (3) In section 85(8)(b) (disclosure of information by Revenue and Customs) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. 35

*Legal Services Act 2007*

- 20 In section 169(3)(b) of the Legal Services Act 2007 (disclosure of information to the Legal Services Board) for “Part 1 of the Regulation of Investigatory

Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.

*Regulatory Enforcement and Sanctions Act 2008*

- 21 In section 70(4) of the Regulatory Enforcement and Sanctions Act 2008 (disclosure of information) for paragraph (b) substitute – 5  
“(b) any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.”

*Counter-Terrorism Act 2008*

- 22 In section 20(2)(b) of the Counter-Terrorism Act 2008 (disclosure and the intelligence services: supplementary provisions) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. 10

*Borders, Citizenship and Immigration Act 2009*

- 23 In section 19(1)(b) of the Borders, Citizenship and Immigration Act 2009 (application of statutory provisions) for “Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. 15

*Marine and Coastal Access Act 2009*

- 24 (1) The Marine and Coastal Access Act 2009 is amended as follows.  
(2) In paragraph 13(5) of Schedule 7 (further provision about civil sanctions under Part 4: disclosure of information) for paragraph (b) substitute – 20  
“(b) any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.”  
(3) In paragraph 9(5) of Schedule 10 (further provision about fixed monetary penalties under section 142: disclosure of information) for paragraph (b) substitute – 25  
“(b) any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.”

*Terrorist Asset-Freezing etc. Act 2010*

- 25 In section 25(2)(b) of the Terrorist Asset-Freezing etc. Act 2010 (application of provisions) for “Part 1 of the Regulation of Investigatory Powers Act 2000” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”. 30

*Marine (Scotland) Act 2010 (2010 asp 5)*

- 26 In paragraph 12(5) of Schedule 2 to the Marine (Scotland) Act 2010 (further provision about civil sanctions under Part 4: disclosure of information) for paragraph (b) substitute – 35  
“(b) any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.”

*Charities Act 2011*

- 27 In section 59(b) of the Charities Act 2011 (disclosure: supplementary) for “Part 1 of the Regulation of Investigatory Powers Act 2000” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.

*Prisons (Interference with Wireless Telegraphy) Act 2012*

5

- 28 In section 4(6) of the Prisons (Interference with Wireless Telegraphy) Act 2012 (meaning of “telecommunication system”) for “Regulation of Investigatory Powers Act 2000” substitute “Investigatory Powers Act 2016 (see section 223(13) of that Act)”.

*Crime and Courts Act 2013*

10

- 29 In paragraph 1(b) of Schedule 7 to the Crime and Courts Act 2013 (information: restrictions on disclosure) for “Part 1 of the Regulation of Investigatory Powers Act 2000” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.

*Marine Act (Northern Ireland) 2013 (c. 10 (N.I.))*

15

- 30 In paragraph 8(5) of Schedule 2 to the Marine Act (Northern Ireland) 2013 (further provision about fixed monetary penalties under section 35: disclosure of information) for paragraph (b) substitute –  
“(b) any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.”

20

*Local Audit and Accountability Act 2014*

- 31 In paragraph 3(3)(b) of Schedule 9 to the Local Audit and Accountability Act 2014 (data matching: voluntary provision of data) for “Part 1 of the Regulation of Investigatory Powers Act 2000” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.

25

*Anti-social Behaviour, Crime and Policing Act 2014*

- 32 In paragraph 7(4)(b) of Schedule 4 to the Anti-social Behaviour, Crime and Policing Act 2014 (ASB case reviews: information) for “Part 1 of the Regulation of Investigatory Powers Act 2000” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.

30

*Immigration Act 2014*

- 33 In paragraph 6(b) of Schedule 6 to the Immigration Act 2014 (information) for “Part 1 of the Regulation of Investigatory Powers Act 2000” substitute “any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016”.

35

*Data Retention and Investigatory Powers Act 2014*

- 34 Omit sections 4(1), 7 and 8 of the Data Retention and Investigatory Powers Act 2014 (introductory, review and final provisions).

PART 2

LAWFUL INTERCEPTION OF COMMUNICATIONS

*Official Secrets Act 1989*

- 35 In section 4(3) of the Official Secrets Act 1989 (crime and special investigation powers) omit the “and” after paragraph (a) and after paragraph (b) insert “and” 5
- (c) any information obtained under a warrant under Chapter 1 of Part 2 or Chapter 1 of Part 6 of the Investigatory Powers Act 2016, any information relating to the obtaining of information under such a warrant and any document or other article which is or has been used or held for use in, or has been obtained by reason of, the obtaining of information under such a warrant.” 10

*Criminal Procedure and Investigations Act 1996*

- 36 (1) The Criminal Procedure and Investigations Act 1996 is amended as follows. 15
- (2) In section 3(7) (initial duty of prosecutor to disclose) for “section 17 of the Regulation of Investigatory Powers Act 2000” substitute “section 48 of the Investigatory Powers Act 2016”.
- (3) In section 7A(9) (continuing duty of prosecutor to disclose) for “section 17 of the Regulation of Investigatory Powers Act 2000 (c. 23)” substitute “section 48 of the Investigatory Powers Act 2016”. 20
- (4) In section 8(6) (application by accused for disclosure) for “section 17 of the Regulation of Investigatory Powers Act 2000” substitute “section 48 of the Investigatory Powers Act 2016”.
- (5) In section 23 (code of practice) for subsection (6) substitute – 25
- “(6) The code must be so framed that it does not apply to any of the following –
- (a) material intercepted in obedience to a warrant issued under section 2 of the Interception of Communications Act 1985;
- (b) material intercepted under the authority of an interception warrant under section 5 of the Regulation of Investigatory Powers Act 2000; 30
- (c) material obtained under the authority of a warrant issued under Chapter 1 of Part 2 of the Investigatory Powers Act 2016; 35
- (d) material obtained under the authority of a warrant issued under Chapter 1 of Part 6 of that Act.”

*Scotland Act 1998*

- 37 In Section B8 of Part 2 of Schedule 5 to the Scotland Act 1998 (reserved matters: national security, interception of communications etc.), in the definition of “private telecommunication system”, for “section 2(1) of the Regulation of Investigatory Powers Act 2000” substitute “section 223(14) of the Investigatory Powers Act 2016”. 40

*Northern Ireland Act 1998*

- 38 In paragraph 17 of Schedule 2 to the Northern Ireland Act 1998 (excepted matters) for paragraph (b) substitute –
- “(b) the subject-matter of sections 2 to 8, Schedule 1, Part 2 and Chapter 1 of Part 6 of the Investigatory Powers Act 2016, except so far as relating to the prevention or detection of serious crime (within the meaning of that Act);”.
- 5

*Financial Services and Markets Act 2000*

- 39 In section 394(7)(a) of the Financial Services and Markets Act 2000 (access to FCA or PRA material) for “section 17 of the Regulation of Investigatory Powers Act 2000” substitute “section 48 of the Investigatory Powers Act 2016”.
- 10

*Regulation of Investigatory Powers Act 2000*

- 40 The Regulation of Investigatory Powers Act 2000 is amended as follows.
- 41 Omit Chapter 1 of Part 1 (interception of communications). 15
- 42 In section 71 (issue and revision of codes of practice) omit subsection (10).
- 43 In section 78(3)(a) (affirmative orders) omit “12(10), 13(3),”.
- 44 (1) Section 81 (general interpretation) is amended as follows.
- (2) In subsection (1) –
- (a) in the definition of “criminal”, omit “or prosecution”, and 20
- (b) in the definition of “interception warrant”, for “a warrant under section 5” substitute “–
- (a) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2 of the Investigatory Powers Act 2016, or 25
- (b) a bulk interception warrant under Chapter 1 of Part 6 of that Act”.
- (3) In subsection (4) omit the words from “; and references” to the end.
- (4) In subsection (5) omit the words from “, except that” to the end.
- 45 In section 82 (amendments, repeals and savings etc.) omit subsections (4) to (6). 30

*Police Reform Act 2002*

- 46 (1) Paragraph 19ZD of Schedule 3 to the Police Reform Act 2002 (handling of complaints and conduct matters etc: restriction on further disclosure of sensitive information) is amended as follows. 35
- (2) In sub-paragraph (2)(b) for “intercept information” substitute “protected information relating to a relevant warrant”.
- (3) In sub-paragraph (4) –
- (a) omit the definitions of “intercept information” and “relevant interception warrant”, 40

- (b) after the definition of “Minister of the Crown” insert –  
     ““protected information”, in relation to a relevant  
     warrant, means information relating to any of the  
     matters mentioned in section 49(4) of the  
     Investigatory Powers Act 2016 in relation to the  
     warrant;”, 5
- (c) in the definition of “relevant authority”, for paragraph (e)  
     substitute –  
     “(e) in the case of protected information relating to a  
     relevant warrant, the person to whom the warrant is  
     or was addressed;”, 10
- (d) at the end insert –  
     ““relevant warrant” means –  
     (a) a warrant under Chapter 1 of Part 2 of the  
     Investigatory Powers Act 2016, or 15  
     (b) a warrant under Chapter 1 of Part 6 of that  
     Act.”

*Criminal Justice and Licensing (Scotland) Act 2010 (2010 asp 13)*

- 47 In section 159 of the Criminal Justice and Licensing (Scotland) Act 2010, for  
     “section 17 of the Regulation of Investigatory Powers Act 2000 (c. 23)” 20  
     substitute “section 48 of the Investigatory Powers Act 2016”.

*Justice and Security Act 2013*

- 48 In section 6(4)(b) of the Justice and Security Act 2013 (declaration permitting  
     closed material applications in proceedings) for sub-paragraph (iii)  
     substitute – 25  
     “(iii) section 48(1) of the Investigatory Powers Act 2016  
     (exclusion for intercept material),”.

PART 3

ACQUISITION OF COMMUNICATIONS DATA

*Regulation of Investigatory Powers Act 2000* 30

- 49 The Regulation of Investigatory Powers Act 2000 is amended as follows.
- 50 Omit Chapter 2 of Part 1 (acquisition and disclosure of communications  
     data).
- 51 In section 49(1)(c) (investigation of electronic data protected by encryption  
     etc: powers under which data obtained) – 35  
     (a) for the words from “section 22(3)” to “Part II” substitute “Part 3 of the  
     Investigatory Powers Act 2016 or Part 2 of this Act”, and  
     (b) for “under section 22(4)” substitute “in pursuance of an authorisation  
     under Part 3 of the Act of 2016 or as the result of the issue of a  
     warrant under Chapter 2 of Part 6 of the Act of 2016”. 40
- 52 In section 71(2) (issue and revision of codes of practice) omit “23A or”.
- 53 (1) Section 77A (procedure for order of sheriff under section 23A or 32A:  
     Scotland) is amended as follows.



- (2) In the heading and in subsection (1) for “section 23A or 32A” substitute “section 32A of this Act or section 66 of the Investigatory Powers Act 2016”.
- (3) In subsection (3) for “sections 23B and 32B and this section” substitute “this section, section 32B of this Act and section 66 of the Investigatory Powers Act 2016”. 5
- 54 (1) Section 77B (procedure for order of district judge under section 23A or 32A: Northern Ireland) is amended as follows.
- (2) In the heading and in subsections (1) and (4) for “section 23A or 32A” substitute “section 32A of this Act or section 66 of the Investigatory Powers Act 2016”. 10
- (3) In subsection (4) for “sections 23B and 32B” substitute “section 32B of this Act and section 66 of that Act”.
- 55 In section 78(3)(a) (affirmative orders) omit “22(9), 23A(6), 25(5),”.
- 56 In section 81(9) (general interpretation: certain references relating to Northern Ireland) omit “23A(7)(b),”. 15

*Police Reform Act 2002*

- 57 (1) Paragraph 19ZA of Schedule 3 to the Police Reform Act 2002 (investigations by the IPCC: information notices) is amended as follows.
- (2) In sub-paragraph (3) omit –
- (a) the words from “(within the meaning of Chapter 2” to “2000)”, and 20
- (b) the words “(within the meaning of that Chapter)”.
- (3) After sub-paragraph (3) insert –
- “(3A) In sub-paragraph (3) “communications data”, “postal operator” and “telecommunications operator” have the same meanings as in the Investigatory Powers Act 2016 (see sections 223 and 224 of that Act).” 25

PART 4

RETENTION OF COMMUNICATIONS DATA

*Anti-terrorism, Crime and Security Act 2001*

- 58 Omit Part 11 of the Anti-terrorism, Crime and Security Act 2001 (retention of communications data). 30

*Data Retention and Investigatory Powers Act 2014*

- 59 Omit sections 1 and 2 of the Data Retention and Investigatory Powers Act 2014 (retention of relevant communications data).

PART 5

EQUIPMENT INTERFERENCE

*Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11)*

- 60 The Regulation of Investigatory Powers (Scotland) Act 2000 is amended as follows. 5
- 61 In section 5(3) (lawful surveillance etc.), after paragraph (a) (and before the “or” at the end of the paragraph), insert—
- “(aa) an enactment contained in Part 5, or Chapter 3 of Part 6, of the Investigatory Powers Act 2016 (equipment interference) so far as relating to the Police Service;” 10
- 62 In section 24(2) (issue and revision of codes of practice), after paragraph (a) (and before the “and” at the end of the paragraph), insert—
- “(aa) Part 5, or Chapter 3 of Part 6, of the Investigatory Powers Act 2016 (equipment interference) so far as relating to the Police Service or the Police Investigations and Review Commissioner;” 15

*Crime and Courts Act 2013*

- 63 (1) In Schedule 1 to the Crime and Courts Act 2013 (the NCA and NCA officers), paragraph 6A (investigatory activity in Northern Ireland) is amended as follows. 20
- (2) In sub-paragraph (3)—
- (a) in the opening words, omit “an authorisation granted under any of the following provisions”;
- (b) before paragraph (a) insert—
- “(za) a targeted equipment interference warrant under Part 5 of the Investigatory Powers Act 2016;” 25
- (c) in paragraph (a), for “in the” substitute “an authorisation granted under any of the following provisions of the”;
- (d) in paragraph (b), at the beginning insert “an authorisation granted under”. 30
- (3) After sub-paragraph (3) insert—
- “(4) For the purpose of sub-paragraph (1), a relevant investigatory activity falling within sub-paragraph (3)(za) is to be regarded as carried out in Northern Ireland if (and to the extent that)—
- (a) the equipment that is being interfered with under the warrant is in Northern Ireland, and 35
- (b) at the time of the carrying out of the activity, the NCA officer knows that the equipment is in Northern Ireland.
- (5) Sub-paragraph (6) applies where—
- (a) in the carrying out by an NCA officer of a relevant investigatory activity falling within sub-paragraph (3)(za), equipment in Northern Ireland is interfered with under the warrant, 40

- (b) at the time the interference begins, the NCA officer does not know that the equipment is in Northern Ireland, and
  - (c) at any time while the interference is continuing, the NCA officer becomes aware that the equipment is in Northern Ireland. 5
- (6) The NCA officer is not to be regarded as in breach of subparagraph (1) if the interference continues after the NCA officer becomes aware that the equipment is in Northern Ireland, provided that the officer informs the Chief Constable of the Police Service of Northern Ireland about the interference as soon as reasonably practicable.” 10

## PART 6

### JUDICIAL COMMISSIONERS

#### *Police Act 1997*

- 64 The Police Act 1997 is amended as follows. 15
- 65 In section 103(8) (appeals) for “the period” substitute “any period”.
- 66 In section 105(1)(b)(iii) (reports of appeals dismissed) for “section 107(2)” substitute “section 201 of the Investigatory Powers Act 2016”.
- 67 In section 108(1) (interpretation of Part 3) after the definition of “designated deputy” insert— 20
- ““the Investigatory Powers Commissioner” and “Judicial Commissioner” have the same meanings as in the Investigatory Powers Act 2016 (see section 225(1) of that Act);”.

#### *Regulation of Investigatory Powers Act 2000* 25

- 68 The Regulation of Investigatory Powers Act 2000 is amended as follows.
- 69 In section 37(9)(a) (appeals against decisions of ordinary Surveillance Commissioners) for “the period” substitute “any period”.
- 70 In section 39(3) (appeals: reports of Chief Surveillance Commissioner)— 30
- (a) for “Subsections (3) and (4) of section 107 of the Police Act 1997” substitute “Subsections (6) to (9) of section 201 of the Investigatory Powers Act 2016”, and
  - (b) for “subsection (2) of that section” substitute “subsection (1) of that section”.
- 71 Omit section 40 (information to be provided to Surveillance Commissioners). 35
- 72 In section 50(7)(b) (notification to Intelligence Services Commissioner or Chief Surveillance Commissioner of certain directions relating to the disclosure of a key to protected information) for “the Commissioner in question” substitute “the Investigatory Powers Commissioner”. 40
- 73 In section 71(2) (issue and revision of codes of practice) for “the Surveillance Commissioners” substitute “a Judicial Commissioner”.

- 
- 74 (1) Section 72 (effect of codes of practice) is amended as follows.
- (2) In subsection (4) for paragraphs (c) to (e) (and the word “or” between paragraphs (d) and (e)) substitute “, or  
“(ba) the Investigatory Powers Commissioner or any other Judicial Commissioner carrying out functions under this Act, the Investigatory Powers Act 2016 or the Police Act 1997,”. 5
- (3) Omit subsection (5).
- 75 (1) Section 81(1) (general definitions) is amended as follows.
- (2) Omit the definitions of “Assistant Surveillance Commissioner”, “ordinary Surveillance Commissioner”, “Surveillance Commissioner” and “Chief Surveillance Commissioner”. 10
- (3) After the definition of “interception warrant” insert –  
““the Investigatory Powers Commissioner” and “Judicial Commissioner” have the same meanings as in the Investigatory Powers Act 2016 (see section 225(1) of that Act);” 15

*Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11)*

- 76 The Regulation of Investigatory Powers (Scotland) Act 2000 is amended as follows.
- 77 In the cross-heading before section 2 (Surveillance Commissioners) for “Surveillance” substitute “Judicial”. 20
- 78 In section 2(10) (restrictions on appeals against Commissioners) –  
(a) for “Chief Surveillance Commissioner” substitute “Investigatory Powers Commissioner”, and  
(b) for “other Surveillance Commissioner” substitute “other Judicial Commissioner”. 25
- 79 In the heading of section 16 for “Surveillance Commissioners” substitute “Judicial Commissioners”.
- 80 Omit section 18 (information to be provided to Surveillance Commissioners). 30
- 81 In the cross-heading before section 21 (Chief Surveillance Commissioner) for “Chief Surveillance” substitute “Investigatory Powers”.
- 82 Omit section 21 (functions of Chief Surveillance Commissioner).
- 83 (1) Section 22 (co-operation with, and reports by, Chief Surveillance Commissioner) is amended as follows. 35
- (2) Omit subsection (1).
- (3) In subsection (2) for “Chief Surveillance Commissioner” substitute “Investigatory Powers Commissioner”.
- (4) In subsection (3) –  
(a) for “Chief Surveillance Commissioner” substitute “Investigatory Powers Commissioner”, and  
(b) after “under” insert “, and in relation to,”. 40

- 84 In section 24(2) (issue and revision of codes of practice) for “the Surveillance Commissioners appointed under this Act or the Commissioners holding office under section 91 of that Act” substitute “the Judicial Commissioners”.
- 85 In section 26(4) (effect of codes of practice) –
- (a) in paragraph (b) for “Chief Surveillance Commissioner” substitute “Investigatory Powers Commissioner”, and
  - (b) in paragraph (c) for “a Surveillance Commissioner” substitute “a Judicial Commissioner (other than the Investigatory Powers Commissioner)”.
- 86 (1) Section 31(1) (interpretation) is amended as follows. 10
- (2) After the definitions of “directed” and “intrusive” insert –
- “the Investigatory Powers Commissioner” and “Judicial Commissioner” have the same meanings as in the Investigatory Powers Act 2016 (see section 225(1) of that Act);”.
- 15
- (3) Omit the definitions of “ordinary Surveillance Commissioner”, “Surveillance Commissioner” and “Chief Surveillance Commissioner”.

*Terrorism Prevention and Investigation Measures Act 2011*

- 87 In section 21(3)(b) of the Terrorism Prevention and Investigation Measures Act 2011 (duty to consult certain persons before making an order for the continuation, repeal etc. of TPIM powers) for “the Intelligence Services Commissioner” substitute “the Investigatory Powers Commissioner”. 20

*Protection of Freedoms Act 2012*

- 88 The Protection of Freedoms Act 2012 is amended as follows.
- 89 (1) Section 29 (code of practice for surveillance camera systems) is amended as follows. 25
- (2) In subsection (5)(d) (duty to consult certain persons in preparing code) for “the Chief Surveillance Commissioner” substitute “the Investigatory Powers Commissioner”.
- (3) In subsection (7) omit the definition of “the Chief Surveillance Commissioner”. 30
- 90 In section 33(8)(d) (duty to consult before making an order identifying who must have regard to the code) for “the Chief Surveillance Commissioner” substitute “the Investigatory Powers Commissioner”.

PART 7

35

OTHER MINOR AND CONSEQUENTIAL PROVISION

*Telecommunications Act 1984*

- 91 Omit section 94 of the Telecommunications Act 1984 (directions in the interests of national security etc.).

*Northern Ireland Act 1998*

- 92 In paragraph 17 of Schedule 2 to the Northern Ireland Act 1998 (excepted matters) after “subversion;” insert “the Technical Advisory Board provided for by section 211 of the Investigatory Powers Act 2016;”.

*Communications Act 2003*

5

- 93 (1) The Communications Act 2003 is amended as follows.
- (2) In section 401(5)(g), for “sections 47 to 49” substitute “section 47 or 48”.
- (3) In Schedule 18 (transitional provisions), omit paragraph 24 (which relates to section 94 of the Telecommunications Act 1984).

PART 8

10

REPEALS AND REVOCATIONS CONSEQUENTIAL ON OTHER REPEALS OR AMENDMENTS IN THIS ACT

*General amendments*

| <i>Title</i>           | <i>Extent of repeal or revocation</i>                          |    |
|------------------------|--|----|
| Serious Crime Act 2015 | Section 83.<br>Section 86(12).<br>In Schedule 4, paragraph 18. | 15 |

*Lawful interception of communications*

| <i>Title</i>  | <i>Extent of repeal or revocation</i> |    |
|---|---------------------------------------|----|
| Regulation of Investigatory Powers Act 2000                 | In Schedule 4, paragraphs 7(2) and 9. | 20 |
| Inquiries Act 2005  | In Schedule 2, paragraphs 20 and 21.  |    |
| Terrorism Act 2006  | Section 32.                           |    |
| Wireless Telegraphy Act 2006                                | In Schedule 7, paragraphs 22 and 23.  |    |
| National Health Service (Consequential Provisions) Act 2006 | In Schedule 1, paragraph 208.         | 25 |
| Armed Forces Act 2006                                       | In Schedule 16, paragraph 169.        |    |
| Serious Crime Act 2007                                      | In Schedule 12, paragraph 6.          |    |
| Counter-Terrorism Act 2008                                  | Sections 69 and 74.                   | 30 |
| Policing and Crime Act 2009                                 | Section 100.                          |    |
| Terrorist Asset-Freezing etc. Act 2010                      | Section 28(2) and (3).                |    |
| Terrorism Prevention and Investigation Measures Act 2011    | In Schedule 7, paragraph 4.           | 35 |



| <i>Title</i>   | <i>Extent of repeal or revocation</i>                       |    |
|--|---|----|
| Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 (S.I. 2011/1340) | The whole Regulations.                                      | 5  |
| Health and Social Care Act 2012  | In Schedule 5, paragraph 98.                                |    |
| Justice and Security Act 2013  | Section 16.<br>In Schedule 2, paragraph 11.                 |    |
| Crime and Courts Act 2013  | In Schedule 8, paragraph 78.                                | 10 |
| Crime and Courts Act 2013 – <i>cont.</i>   | In Schedule 9, paragraph 125.                               |    |
| Data Retention and Investigatory Powers Act 2014   | Section 3(1) and (2).<br>Section 4(2) to (7).<br>Section 5. | 15 |
| Counter-Terrorism and Security Act 2015  | Section 15(3).<br>In Schedule 8, paragraph 2.               |    |

*Acquisition of communications data*

| <i>Title</i>   | <i>Extent of repeal or revocation</i>   |    |
|--|---|----|
| Serious Organised Crime and Police Act 2005  | In Schedule 4, paragraph 135.   | 20 |
| Serious Crime Act 2007   | In Schedule 12, paragraphs 7 and 8.   |    |
| Police, Public Order and Criminal Justice (Scotland) Act 2006 (Consequential Provisions and Modifications) Order 2007 (S.I. 2007/1098) | In the Schedule, paragraph 4(5).  | 25 |
| Policing and Crime Act 2009  | Section 7.<br>In Schedule 7, paragraphs 13 and 14.  | 30 |
| Protection of Freedoms Act 2012  | Section 37.<br>In Schedule 9, paragraphs 7 and 8 and, in paragraph 16(b), sub-paragraph (i) (and the word “and” at the end of sub-paragraph (i)). |    |
| Crime and Courts Act 2013  | In Schedule 8, paragraph 81.  | 35 |
| Police and Fire Reform (Scotland) Act 2012 (Consequential Provisions and Modifications) Order 2013 (S.I. 2013/602)                     | In Schedule 2, paragraph 33(5) to (8) and (15)(a).  | 40 |
| Data Retention and Investigatory Powers Act 2014   | Section 3(3) and (4).<br>Section 4(8) to (10).  |    |
| Counter-Terrorism and Security Act 2015  | Section 21.<br>Section 52(3)(a).  | 45 |

*Judicial Commissioners*

| <i>Title</i>   | <i>Extent of repeal or revocation</i>  |    |
|--|--|----|
| Scotland Act 1998 (Cross-Border Public Authorities) (Adaptation of Functions etc.) Order 1999 (S.I. 1999/1747)     | In Schedule 6, paragraph 2(2) and (5).   | 5  |
| Regulation of Investigatory Powers Act 2000  | In Schedule 4, paragraph 8(1), (10) and (11).                                  |    |
| Insolvency Act 2000  | In Schedule 4, paragraph 22(2).  | 10 |
| Insolvency Act 2000 (Company Directors Disqualification Undertakings) Order 2004 (S.I. 2004/1941)                  | In the Schedule, paragraph 10.   |    |
| Scotland Act 1998 (Transfer of Functions to the Scottish Ministers etc.) (No 2) Order 2000 (S.I. 2000/3253)        | In Schedule 3, paragraphs 9 to 12.   | 15 |
| Constitutional Reform Act 2005   | In Schedule 17, paragraphs 27 and 30(2)(a) and (b) and (3).                    | 20 |
| Tribunals, Courts and Enforcement Act 2007   | In Schedule 16, paragraph 11(2).   |    |
| Serious Crime Act 2007   | In Schedule 12, paragraph 3.   |    |
| Companies Act 2006 (Consequential Amendments, Transitional Provisions and Savings) Order 2009 (S.I. 2009/1941)     | In Schedule 1, paragraph 169.  | 25 |
| Police Reform and Social Responsibility Act 2011   | In Schedule 16, paragraph 222.   | 30 |
| Protection of Freedoms Act 2012  | In Schedule 9, paragraphs 10 and 11.   |    |
| Justice and Security Act 2013  | Section 5.<br>In Schedule 2, paragraph 4.                                      |    |
| Crime and Courts Act 2013  | In Schedule 8, paragraph 59.<br>In Schedule 21, paragraph 4.                   | 35 |
| Police and Fire Reform (Scotland) Act 2012 (Consequential Provisions and Modifications) Order 2013 (S.I. 2013/602) | In Schedule 1, paragraph 6(6).<br>In Schedule 2, paragraph 33(20) and (22)(c). | 40 |
| Anti-social Behaviour, Crime and Policing Act 2014   | Section 150.   |    |
| Data Retention and Investigatory Powers Act 2014   | Section 6.   | 45 |

*Other minor and consequential provision*

| <i>Title</i>            | <i>Extent of repeal or revocation</i> |
|-------------------------|---------------------------------------|
| Communications Act 2003 | In Schedule 17, paragraph 70.         |

---

# Investigatory Powers Bill

---

---

A

## B I L L

To make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.

*Presented by Secretary Theresa May,  
supported by the Prime Minister,  
Secretary Philip Hammond,  
Secretary Michael Fallon,  
Secretary David Mundell,  
Secretary Theresa Villiers,  
the Attorney General,  
Robert Buckland and  
Mr John Hayes.*

---

*Ordered, by The House of Commons,  
to be Printed, 1 March 2016.*

---

© Parliamentary copyright House of Commons 2016

*This publication may be reproduced under the terms of the Open Parliament Licence, which is published at  
[www.parliament.uk/site-information/copyright](http://www.parliament.uk/site-information/copyright)*

PUBLISHED BY AUTHORITY OF THE HOUSE OF COMMONS  
LONDON – THE STATIONERY OFFICE LIMITED  
Printed in the United Kingdom by The Stationery Office Limited  
£x.xx