THE DATA RETENTION AND ACQUISITION REGULATIONS

Keeling Schedule for amendments to the Investigatory Powers Act 2016

INVESTIGATORY POWERS ACT 2016
Part 1

General Privacy Protections

[Section 1 unchanged]

2. General duties in relation to privacy

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

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

(b) to modify such a warrant,

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

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

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

(f) to vary or revoke such a notice,

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

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

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

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

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

(2) The public authority must have regard to—

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

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

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

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

(3) The duties under subsection (2)—

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

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

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

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

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

(c) other considerations which are relevant to—

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

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

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

(e) other requirements of public law.

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

(a) items subject to legal privilege,

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

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

(6) […]

[Sections 3 to 14 unchanged]

Part 3

Authorisations for Obtaining Communications Data

Targeted authorisations for obtaining data: the Investigatory Powers Commissioner

60A. Power of Investigatory Powers Commissioner to grant authorisations

(1) Subsection (2) applies where the Investigatory Powers Commissioner, on an application made by a relevant public authority, considers—

(a) that it is necessary for the relevant public authority to obtain communications data for a purpose falling within subsection (7),

(b) that it is necessary for the relevant public authority to obtain the data—

(i) for the purposes of a specific investigation or a specific operation, or

(ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, and

(c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.

(2) The Investigatory Powers Commissioner may authorise the relevant public authority to engage in any conduct which—

(a) is for the purpose of obtaining the data from any person, and

(b) relates to—

(i) a telecommunication system, or

(ii) data derived from a telecommunication system.

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

(a) section 62 (restrictions in relation to internet connection records),

(b) sections 70, 73 and 75 and Schedule 4 (restrictions relating to certain relevant public authorities),

(c) section 76 (requirement to consult a single point of contact), and

(d) section 77 (Commissioner approval for authorisation to identify or confirm journalistic sources).

(4) Authorised conduct may, in particular, consist of the relevant public authority—

(a) obtaining the communications data itself from any person or telecommunication system,

(b) asking any person whom the relevant public authority believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it), and

(ii) to disclose the data (whether already in the person's possession or subsequently obtained by that person) to the relevant public authority, or

(c) requiring by notice a telecommunications operator whom the relevant public authority believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it), and

(ii) to disclose the data (whether already in the operator's possession or subsequently obtained by the operator) to the relevant public authority.

(5) An authorisation—

(a) may relate to data whether or not in existence at the time of the authorisation,

(b) may authorise the obtaining or disclosure of data by a person other than the relevant public authority, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned, and

(c) may, in particular, require a telecommunications operator who controls or provides a telecommunications 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 may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system.

(7) It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data—

(a) in the interests of national security,

(b) for the applicable crime purpose (see subsection (8)),

(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 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,

(f) to assist investigations into alleged miscarriages of justice, or

(g) 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 reasons for P's death or condition.

(8) In subsection (7)(b), "the applicable crime purpose" means—

(a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime;

(b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.

(9) The fact that the communications data which would be obtained in pursuance of an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that it is necessary to obtain the data for a purpose falling within subsection (7).

(10) See—

(a) sections 70 and 73 for the meaning of "relevant public authority";

(b) section 84 for the way in which this Part applies to postal operators and postal services;

(c) section 86(2A) for the meaning of "serious crime".

Targeted authorisations for obtaining data: designated senior officers

61. Power of designated senior officers to grant authorisations

(1) Subsection (2) applies if a designated senior officer of a relevant public authority considers—

(a) that it is necessary to obtain communications data for a purpose falling within subsection (7),

(b) that it is necessary to obtain the data—

(i) for the purposes of a specific investigation or a specific operation, or

(ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, and

(c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.

(2) The designated senior officer may authorise any officer of the authority to engage in any conduct which—

(a) is for the purpose of obtaining the data from any person, and

(b) relates to—

(i) a telecommunication system, or

(ii) data derived from a telecommunication system.

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

(a) section 62 (restrictions in relation to internet connection records),

(b) section 63 (additional restrictions on grant of authorisations),

(c) sections 70, 73 and 75 and Schedule 4 (restrictions relating to certain relevant public authorities),

(d) section 76 (requirement to consult a single point of contact), and

(e) section 77 (Commissioner approval for authorisations to identify or confirm journalistic sources).

(4) Authorised conduct may, in particular, consist of an authorised officer—

(a) obtaining the communications data themselves from any person or telecommunication system,

(b) asking any person whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it), and

(ii) to disclose that data (whether already in the person's possession or subsequently obtained by that person) to a person identified by, or in accordance with, the authorisation, or

(c) requiring by notice a telecommunications operator whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it), and

(ii) to disclose the data (whether already in the person's possession or subsequently obtained by that person) to a person identified by, or in accordance with, the authorisation.

(5) An authorisation—

(a) may relate to data whether or not in existence at the time of the authorisation,

(b) may authorise the obtaining or disclosure of data by a person who is not an authorised officer, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned, and

(c) may, in particular, require a telecommunications operator who controls or provides a telecommunications system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system.

(6) An authorisation—

(a) may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunications system, and

(b) may not authorise an authorised officer to ask or require, in the circumstances mentioned in subsection (4)(b) or (c), a person to disclose the data to any person other than—

(i) an authorised officer, or

(ii) an officer of the same relevant public authority as an authorised officer.

(7) It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data—

(a) in the interests of national security,

(b) for the applicable crime purpose (see subsection (7A)),

(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), (e), (f), (g), (h), (i), (j) […].

(7A) In subsection (7)(b), "the applicable crime purpose" means—

(a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime;

(b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.

(8) The fact that the communications data which would be obtained in pursuance of an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that it is necessary to obtain the data for a purpose falling within subsection (7).

(9) See—

(a) sections 70 and 73 for the meaning of "designated senior officer" and "relevant public authority";

(b) section 84 for the way in which this Part applies to postal operators and postal services;

(c) section 86(2A) for the meaning of "serious crime".

61A. Power of designated officers to grant authorisations: urgent cases

(1) Subsection (2) applies if a designated senior officer of a relevant public authority considers—

(a) that it is necessary to obtain communications data for a purpose falling within subsection (7),

(b) that it is necessary to obtain the data for the purposes of a specific investigation or a specific operation,

(c) that there is an urgent need to obtain the data, and

(d) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.

(2) The designated senior officer may authorise any officer of the relevant public authority to engage in any conduct which—

(a) is for the purpose of obtaining the data from any person, and

(b) relates to—

(i) a telecommunication system, or

(ii) data derived from a telecommunication system.

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

(a) section 62 (restrictions in relation to internet connection records),

(b) sections 70, 73 and 75 and Schedule 4 (restrictions relating to certain relevant public authorities),

(c) section 76 (requirement to consult a single point of contact), and

(d) section 77 (Commissioner approval for authorisations to identify or confirm journalistic sources).

(4) Authorised conduct may, in particular, consist of an authorised officer—

(a) obtaining the communications data themselves from any person or telecommunication system,

(b) asking any person whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it), and

(ii) to disclose the data (whether already in the person's possession or subsequently obtained by that person) to a person identified by, or in accordance with, the authorisation, or

(c) requiring by notice a telecommunications operator whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it), and

(ii) to disclose the data (whether already in the operator's possession or subsequently obtained by the operator) to a person identified by, or in accordance with, the authorisation.

(5) An authorisation—

(a) may relate to data whether or not in existence at the time of the authorisation,

(b) may authorise the obtaining or disclosure of data by a person who is not an authorised officer, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned, and

(c) may, in particular, require a telecommunications operator who controls or provides a telecommunications system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system.

(6) An authorisation—

(a) may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system, and

(b) may not authorise an authorised officer to ask or require, in the circumstances mentioned in subsection (4)(b) or (c), a person to disclose the data to any person other than—

(i) an authorised officer, or

(ii) an officer of the same relevant public authority as an authorised officer.

(7) It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data—

(a) for the applicable crime purpose (see subsection (8)),

(b) in the interests of public safety,

(c) 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 person's physical or mental health,

(d) to assist investigations into alleged miscarriages of justice, or

(e) 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 concerned with P or about reasons for P's death or condition.

(8) In subsection (7)(a), "the applicable crime purpose" means—

(a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime;

(b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.

(9) The fact that the communications data which would be obtained in pursuance of an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that it is necessary to obtain the data for a purpose falling within subsection (7).

(10) See—

(a) sections 70 and 73 for the meanings of "designated senior officer" and "relevant public authority";

(b) section 84 for the way in which this Part applies to postal operators and postal services;

(c) section 86(2A) for the meaning of "serious crime".

Further provision about authorisations

62. Restrictions in relation to internet connection records

(A1) The Investigatory Powers Commissioner may not, on the application of a local authority, grant an authorisation under section 60A for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record.

(A2) The Investigatory Powers Commissioner may not, on the application of a relevant public authority which is not a local authority, grant an authorisation under section 60A for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record unless condition A, B or C is met.

(1) […]

(2) A designated senior officer of a relevant public authority which is not a local authority may not grant an authorisation for the purposes of obtaining data which is, or can only be obtained by processing, an internet connection record unless condition A, B, or C is met.

(3) Condition A is that the person with power to grant the authorisation considers that it is necessary, for a purpose falling within section 60A(7), 61(7) or 61A(7) (as applicable) to obtain the data to identify which person or apparatus is using an internet service where—

(a) the service and time of use are already known, but

(b) the identity of the person or apparatus using the service is not known.

(4) Condition B is that—

(a) the purpose for which the data is to be obtained falls within section 60A(7), 61(7) or 61A(7) (as applicable) but is not the purpose of preventing or detecting serious crime mentioned in section 60A(8)(a), 61(7A)(a) or 61A(8)(a) or the purpose of preventing or detecting crime mentioned in section 60A(8)(b), 61(7A)(b) or 61A(8)(b), and

(b) the person with the power to grant the authorisation considers that it is necessary to obtain the data to identify—

(i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known,

(ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime, or

(iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(5) Condition C is that—

(a) the purpose for which the data is to be obtained is the purpose of preventing or detecting serious crime mentioned in section 60A(8)(a), 61(7A)(a) or 61A(8)(a) or the purpose of preventing or detecting crime mentioned in section 60A(8)(b), 61(7A)(b) or 61A(8)(b);

(b) the crime to be prevented or detected is relevant crime (see subsection (6)), and

(c) the person with power to grant the authorisation considers that it is necessary to obtain the data to identify—

(i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known,

(ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime, or

(iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(6) In subsection (5), "relevant crime" means serious crime within the meaning of this Part except that it does not include crime which has that meaning only by virtue of section 86(2A)(a) if the offence referred to in that paragraph is one for which the maximum sentence of imprisonment is less than 12 months.

(7) In this Act "internet connection record" means communications data which—

(a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

(b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

63. Additional restrictions on grant of authorisations under section 61

(1) A designed senior officer may not grant an authorisation under section 61 for the purposes of a specific investigation or a specific operation if the officer is working on that investigation or operation.

(2) But, if the designated senior officer considers that there are exceptional circumstances which mean that subsection (1) should not apply in a particular case, that subsection does not apply in that case.

(3) Examples of exceptional circumstances include—

(a) an imminent threat to life or another emergency,

(b) the investigation or operation concerned is one where there is an exceptional need, in the interests of national security, to keep knowledge of it to a minimum, or

(c) there is an opportunity to obtain information where—

(i) the opportunity is rare,

(ii) the time to act is short, and

(iii) the need to obtain the information is significant and in the interests of national security.

(d) […]

64. Procedure for authorisations and authorised notices

(1) An authorisation must specify—

(a) […]

(aa) whether the authorisation has been granted by the Investigatory Powers Commissioner under section 60A or by a designated senior officer under section 61 or 61A,

(b) the matters falling within section 60A(7), 61(7) or 61A(7) (as applicable) by reference to which it is granted,

(c) the conduct that is authorised,

(d) the data or description of data to be obtained, and

(e) the person or descriptions of persons to whom the data is to be, or may be, disclosed or how to identify such persons.

(1A) An authorisation granted by a designated senior officer under section 61 or 61A must also specify the office, rank or position held by the officer.

(2) An authorisation which authorises a person to impose requirements by notice on a telecommunications operator must also specify—

(a) the operator concerned, and

(b) the nature of the requirements that are to be imposed,

but need not specify the other contents of the notice.

(3) The notice itself—

(a) must specify—

(i) the office, rank or position held by the person giving it,

(ii) the requirements that are being imposed, and

(iii) the telecommunications operator on whom the requirements are being imposed, and

(b) must be given in writing or (if not in writing) in a manner that produces a record of its having been given.

(4) An authorisation must be applied for, and granted, in writing or (if not in writing) in a manner that produces a record of its having been applied for or granted.

65. Duration and cancellation of authorisations and notices

(1) An authorisation under section 60A or 61 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 under section 60A or 61 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.

(3A) An authorisation under section 61A ceases to have effect at the end of the period of 3 days beginning with the date on which it is granted.

(3B) Where the Investigatory Powers Commissioner has granted an authorisation under section 60A to a relevant public authority—

(a) the Investigatory Powers Commissioner or an officer of the authority may cancel it at any time, and

(b) the Investigatory Powers Commissioner or an officer of the authority must cancel it if the Commissioner or (as the case may be) the officer considers that the requirements of this Part would not be satisfied in relation to granting an equivalent new authorisation.

(4) A designated senior officer who has granted an authorisation under section 61 or 61A—

(a) may cancel it at any time, and

(b) must cancel it if the designated senior officer considers that the requirements of this Part would not be satisfied in relation to granting an equivalent new authorisation.

(5) The Secretary of State may by regulations provide for the person by whom any function under subsection (4) is to be exercised where the person who would otherwise have exercised it is no longer available to do so.

(6) Such regulations may, in particular, provide for the person by whom the function is to be exercised to be a person appointed in accordance with the regulations.

(7) A notice given in pursuance of an authorisation (and any requirement imposed by the notice)—

(a) is not affected by the authorisation subsequently ceasing to have effect under subsection (1) or (3A), but

(b) is cancelled if the authorisation is cancelled under subsection (3B) or (4).

[Section 66 unchanged]

Filtering arrangements for obtaining data

67. Filtering arrangements for obtaining data.

(1) The Secretary of State may establish, maintain and operate arrangements for the purposes of—

(a) assisting a person, who is considering whether to grant an authorisation, to determine whether the requirements of this Part in relation to granting the authorisation are satisfied, or

(b) facilitating the lawful, efficient and effective obtaining of communications data from any person by relevant public authorities in pursuance of an authorisation.

(2) Arrangements under subsection (1) ("filtering arrangements") may, in particular, involve the obtaining of communications data in pursuance of an authorisation ("the target data") by means of—

(a) a request to the Secretary of State to obtain the target data on behalf of an authorised officer, and

(b) the Secretary of State—

(i) obtaining the target data or data from which the target data may be derived,

(ii) processing the target data or the data from which it may be derived (and retaining data temporarily for that purpose), and

(iii) disclosing the target data to the person identified for this purpose by, or in accordance with, the authorisation.

(3) Filtering arrangements may, in particular, involve the generation or use by the Secretary of State of information—

(a) for the purpose mentioned in subsection (1)(a), or

(b) for the purposes of—

(i) the support, maintenance, oversight, operation or administration of the arrangements, or

(ii) the functions of the Investigatory Powers Commissioner mentioned in subsection (4) or (5).

(4) Filtering arrangements must involve the generation and retention of such information or documents as the Investigatory Powers Commissioner considers appropriate for the purposes of the functions of the Commissioner under section 229(1) of keeping under review the exercise by public authorities of functions under this Part.

(5) The Secretary of State must consult the Investigatory Powers Commissioner about the principles on the basis of which the Secretary of State intends to establish, maintain or operate any arrangements for the purpose mentioned in subsection (1)(a).

68. Use of filtering arrangements in pursuance of an authorisation

(1) This section applies in relation to the use of the filtering arrangements in pursuance of an authorisation.

(2) The filtering arrangements may be used—

(a) to obtain and disclose communications data in pursuance of an authorisation, only if the authorisation specifically authorises the use of the arrangements to obtain and disclose the data,

(b) to process data in pursuance of an authorisation (and to retain the data temporarily for that purpose), only if the authorisation specifically authorises processing data of that description under the arrangements (and their temporary retention for that purpose).

(3) An authorisation must record the decision of the person granting the authorisation as to—

(a) whether the communications data to be obtained and disclosed in pursuance of the authorisation may be obtained and disclosed by use of the filtering arrangements,

(b) whether the processing of data under the filtering arrangements (and its temporary retention for that purpose) is authorised,

(c) if the processing of data under the filtering arrangements is authorised, the description of data that may be processed.

(4) A person must not grant an authorisation which authorises—

(a) use of the filtering arrangements, or

(b) processing under the filtering arrangements,

unless the condition in subsection (5) is met.

(5) The condition is that the person (as well as considering that the other requirements of this Part in relation to granting the authorisation are satisfied) considers that what is authorised in relation to the filtering arrangements is proportionate to what is sought to be achieved.

69. Duties in connection with operation of filtering arrangements

(1) The Secretary of State must secure—

(a) that no authorisation data is obtained or processed under the filtering arrangements except for the purposes of an authorisation,

(b) that data which—

(i) has been obtained or processed under the filtering arrangements, and

(ii) is to be disclosed in pursuance of an authorisation or for the purpose mentioned in section 67(1)(a),

is disclosed only to the person to whom the data is to be disclosed in pursuance of the authorisation […],

(c) that any authorisation data which is obtained under the filtering arrangements in pursuance of an authorisation is immediately destroyed—

(i) when the purposes of the authorisation have been met, or

(ii) if at any time it ceases to be necessary to retain the data for the purposes or purpose concerned.

(2) The Secretary of State must secure that data (other than authorisation data) which is retained under the filtering arrangements is disclosed only—

(a) for the purpose mentioned in section 67(1)(a),

(b) for the purposes of support, maintenance, oversight, operation or administration of the arrangements,

(c) to the Investigatory Powers Commissioner for the purposes of the functions of the Commissioner mentioned in section 67(4) or (5), or

(d) otherwise as authorised by law.

(3) The Secretary of State must secure that—

(a) only the Secretary of State and designated individuals are permitted to read, obtain or otherwise process data for the purposes of support, maintenance, oversight, operation or administration of the filtering arrangements, and

(b) no other persons are permitted to access or use the filtering arrangements except in pursuance of an authorisation or for the purpose mentioned in section 67(1)(a).

(4) In subsection (3)(a) "designated" means designated by the Secretary of State; and the Secretary of State may designate an individual only if the Secretary of State thinks that it is necessary for the individual to be able to act as mentioned in subsection (3)(a).

(5) The Secretary of State must—

(a) put in place and maintain an adequate security system to govern access to, and use of, the filtering arrangements and to protect against any abuse of the power of access, and

(b) impose measures to protect against unauthorised or unlawful data retention, processing, access or disclosure.

(6) The Secretary of State must—

(a) put in place and maintain procedures (including the regular testing of relevant software and hardware) to ensure that the filtering arrangements are functioning properly, and

(b) report, as soon as possible after the end of each calendar year, to the Investigatory Powers Commissioner about the functioning of the filtering arrangements during that year.

(7) A report under subsection (6)(b) must, in particular, contain information about the destruction of authorisation data during the calendar year concerned.

(8) If the Secretary of State believes that significant processing errors have occurred giving rise to a contravention of any of the requirements of this Part which relate to the filtering arrangements, the Secretary of State must report that fact immediately to the Investigatory Powers Commissioner.

(9) In this section "authorisation data", in relation to an authorisation, means communications data that is, or is to be, obtained in pursuance of the authorisation or any data from which that data is, or may be, derived.

Relevant public authorities other than local authorities

70. Relevant public authorities and designated senior officers etc

(1) Schedule 4 (relevant public authorities and designated senior officers etc) has effect.

(2) A public authority listed in column 1 of the table in the Schedule is a relevant public authority for the purposes of this Part.

(2A) An authorisation under section 60A may be granted on the application of a relevant public authority listed in column 1 of the table only if section 60A(1)(a) is met in relation to a purpose within one of the paragraphs of section 60A(7) specified in the corresponding entry in column 2 of the table.

(3) In this Part "designated senior officer", in relation to a 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 3 of the table, or

(b) an office, rank or position higher than that specified in relation to the authority in column 3 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 3 of the table is specified by reference to—

(a) a particular branch, agency or other part of the authority, or

(b) responsibility for functions of a particular description.

(5) A person is a designated senior officer by virtue of subsection (3)(b) only if the person—

(a) holds an office, rank or position in that branch, agency or part, or

(b) has responsibility for functions of that description.

(5A) A person who is a designated senior officer of a relevant public authority by virtue of subsection (3) and an entry in column 3 of the table may grant an authorisation under section 61—

(a) only for obtaining communications data of the kind specified in the corresponding entry in column 4 of the table,

(b) only if one or more paragraphs of section 61(7) is specified in the corresponding entry in column 5 of the table, and

(c) only if section 61(1)(a) is met in relation to a purpose within the specified paragraph or, if more than one paragraph is specified, a purpose within one of them.

(6) A person who is a designated senior officer of a relevant public authority by virtue of subsection (3) and an entry in column 3 of the table may grant an authorisation under section 61A—

(a) only for obtaining communications data of the kind specified in the corresponding entry in column 4 of the table, and

(b) only if one or more paragraphs of section 61A(7) is specified in the corresponding entry in column 6 of the table, and

(c) only if section 61A(1)(a) is met in relation to a purpose within the specified paragraph or, if more than one paragraph is specified, a purpose within one of them.

(7) Where there is more than one entry in relation to a relevant public authority in column 3 of the table, and a person is designated senior officer of the authority by virtue of subsection (3) as it applies to more than one of those entries, subsections (5A) and (6) apply in relation to each entry.

71. Power to modify section 70 and Schedule 4

(1) The Secretary of State may by regulations modify section 70 or Schedule 4.

(2) Regulations under subsection (1) may in particular—

(a) add a public authority to, or remove a public authority from, the list in column 1 of the table,

(b) modify an entry in column 2 of the table,

(c) impose or remove restrictions on the authorisations that may be granted […],

(d) impose or remove restrictions on the circumstances in which or purposes for which the authorisations may be granted.

(2A) Regulations adding a public authority to, or removing a public authority from, the list in column 1 of the table may do so in relation to all or any of the following—

(a) authorisations under section 60A by the Investigatory Powers Commissioner;

(b) authorisations by a designated senior officer under section 61;

(c) authorisations by a designated senior officer under section 61A.

(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 (in relation to one or more of the authorisations mentioned in subsection (2A)) because of regulations under that subsection.

72. Certain regulations under section 71: supplementary

(1) This section applies to regulations under section 71 other than regulations which do only one or both of the following—

(a) remove a public authority from the list in column 1 of the table in Schedule 4 (in relation to one or more of the authorisations mentioned in section 71(2A)) and make consequential modifications,

(b) modify column 3 of the table in a way that does not involve replacing an office, rank or position specified in that column in relation to a particular public authority with a lower office, rank or position in relation to the same authority.

(2) Before making regulations to which this section applies, the Secretary of State must consult—

(a) the Investigatory Powers Commissioner, and

(b) the public authority to which the modifications relate.

(3) A statutory instrument containing regulations to which this section applies may not be made except in accordance with the enhanced affirmative procedure.

Local authorities

73. Local authorities as relevant public authorities

(1) A local authority is a relevant public authority for the purposes of this Part but only so far as relating to authorisations under section 60A.

(2) […]

(3) An authorisation may not be granted under section 60A on the application of a local authority unless—

(a) section 60A(1)(a) is met in relation to a purpose within section 60A(7)(b),

(b) the local authority is a party to a collaboration agreement (whether as a supplying authority or a subscribing authority or both), and

(c) that collaboration agreement is certified by the Secretary of State (having regard to guidance given by virtue of section 79(6) and (7)) as being appropriate for the local authority.

(3A) In subsection (3), "collaboration agreement", "subscribing authority" and "supplying authority" have the same meaning as in section 78.

(4), (5), (6), (7) […]

74. […]

75. […]

Additional protections

76. Use of a single point of contact

(A1) Before making an application for an authorisation under section 60A, the officer making the application must consult a person who is acting as a single point of contact in relation to the making of applications.

(1) Before granting an authorisation under section 61 or 61A, the designated senior officer must consult a person who is acting as a single point of contact in relation to the granting of authorisations.

(2) But, if the officer or (as the case may be) designated senior officer considers that there are exceptional circumstances which mean that subsection (A1) or (as the case may be) (1) should not apply in a particular case, that subsection does not apply in that case.

(3) Examples of exceptional circumstances include—

(a) an imminent threat to life or another emergency, or

(b) the interests of national security.

(4) A person is acting as a single point of contact if that person—

(a) is an officer of a relevant public authority, and

(b) is responsible for advising—

(i) officers of the relevant public authority about applying for authorisations (whether under section 60A, 61 or 61A), or

(ii) designated senior officers of the relevant public authority about granting authorisations.

(5) A person acting as a single point of contact may, in particular, advise an officer of a relevant public authority who is considering whether to apply for an authorisation about—

(a) the most appropriate methods for obtaining data where the data concerned is processed by more than one telecommunications operator,

(b) the cost, and resource implications, for—

(i) the relevant public authority concerned of obtaining the data, and

(ii) the telecommunications operator concerned of disclosing the data,

(c) any unintended consequences of the proposed authorisation, and

(d) any issues as to the lawfulness of the proposed authorisation.

(6) A person acting as a single point of contact may, in particular, advise a designated senior officer who is considering whether to grant an authorisation about—

(a) whether it is reasonably practical to obtain the data sought in pursuance of the proposed authorisation,

(b) the cost, and resource implications, for—

(i) the relevant public authority concerned of obtaining the data, and

(ii) the telecommunications operator concerned of disclosing the data,

(c) any unintended consequences of the proposed authorisation, and

(d) any issues as to the lawfulness of the proposed authorisation.

(7) A person acting as a single point of contact may also provide advice about—

(a) whether requirements imposed by virtue of an authorisation have been met,

(b) the use in support of operations or investigations of communications data obtained in pursuance of an authorisation, and

(c) any other effects of an authorisation.

(8) Nothing in this section prevents a person acting as a single point of contact from also applying for, or being granted, an authorisation or, in the case of a designated senior officer, granting an authorisation.

77. Commissioner approval for authorisations to identify or confirm journalistic sources

(1) Subsection (2) applies if —

(a) a designated senior officer has granted an authorisation under section 61 or 61A in relation to the obtaining by a relevant public authority of communications data for the purpose of identifying or confirming a source of journalistic information, and

(b) the authorisation is not necessary because of an imminent threat to life.

(1A) Subsection 2 also applies if —

(a) a person to whom functions under section 60A have been delegated under section 238(5) has granted an authorisation under that section in relation to the obtaining by a relevant public authority of communications data for the purpose of identifying or confirming a source of journalistic information, and

(b) the authorisation is not necessary because of an imminent threat to life.

(2) The authorisation is not to take effect until such time (if any) as a Judicial Commissioner has approved it.

(3) The relevant public authority for which the authorisation has been granted may apply to a Judicial Commissioner for approval of the authorisation.

(4) The applicant is not required to give notice of the application to—

(a) any person to whom the authorisation relates, or

(b) that person's legal representatives.

(5) A Judicial Commissioner may approve the authorisation if, and only if, the Judicial Commissioner considers that—

(a) at the time of the grant, there were reasonable grounds for considering that the requirements of this Part were satisfied in relation to the authorisation, and

(b) at the time when the Judicial Commissioner is considering the matter, there are reasonable grounds for considering that the requirements of this Part would be satisfied if an equivalent new authorisation were granted at that time.

(6) In considering whether the position is as mentioned in subsection (5)(a) and (b), the Judicial Commissioner must, in particular, have regard to—

(a) the public interest in protecting a source of journalistic information, and

(b) the need for there to be another overriding public interest before a relevant public authority seeks to identify or confirm a source of journalistic information.

(7) Where, on an application under this section, the Judicial Commissioner refuses to approve the grant of the authorisation, the Judicial Commissioner may quash the authorisation.

Collaboration agreements

78. Collaboration agreements

(1) A collaboration agreement is an agreement (other than a police collaboration agreement) under which—

(a) a relevant public authority ("the supplying authority") puts the services of […] officers of that authority at the disposal of another relevant public authority ("the

subscribing authority") for the purposes of the subscribing authority's functions under this Part, and

(b) officers of the supplying authority act as single points of contact for officers of the subscribing authority.

(2) The persons who may act as single points of contact under a collaboration agreement are additional to those persons who could otherwise act as single points of contact.

(3), (4) […]

(5) Where officers of the supplying authority act as single points of contact for officers of the subscribing authority, section 76(4)(b) has effect as if the references to the relevant public authority were references to the subscribing authority.

(6) In this section—

"force collaboration provision" has the meaning given by paragraph (a) of section 22A(2) of the Police Act 1996 but as if the reference in that paragraph to a police force included the National Crime Agency,

"police collaboration agreement" means a collaboration agreement under section 22A of the Police Act 1996 which contains force collaboration provision.

79. Collaboration agreements: supplementary

(1) A collaboration agreement may provide for payments to be made between parties to the agreement.

(2) A collaboration agreement—

(a) must be in writing,

(b) may be varied by a subsequent collaboration agreement, and

(c) may be brought to an end by agreement between the parties to it.

(3) A person who makes a collaboration agreement must—

(a) publish the agreement, or

(b) publish the fact that the agreement has been made and such other details about it as the person considers appropriate.

(4) A relevant public authority may enter into a collaboration agreement as a supplying authority, a subscribing authority or both (whether or not it would have power to do so apart from this section).

(5) The Secretary of State may, after consulting a relevant public authority, direct it to enter into a collaboration agreement if the Secretary of State considers that entering into the agreement would assist the effective exercise by the authority, or another relevant public authority, of its functions under this Part.

(6) A code of practice under Schedule 7 must include guidance to relevant public authorities about collaboration agreements.

(7) The guidance must include guidance about the criteria the Secretary of State will use in considering whether a collaboration agreement is appropriate for a relevant public authority.

80. Police collaboration agreements

(1) This section applies if—

(a) the chief officer of police of an England and Wales police force ("force 1") has entered into a police collaboration agreement for the purposes of a collaborating police force's functions under this Part, and

(b) under the terms of the agreement, officers of force 1 act as single points of contact for officers of the collaborating police force.

(2) The persons who may act as single points of contact under a collaboration agreement are additional to those persons who could otherwise act as single points of contact.

(3), (4) […]

(5) Where officers of force 1 act as single points of contact for officers of the collaborating police force, section 76(4)(b) has effect as if the references to the relevant public authority were references to the collaborating police force.

(6) In this section—

"collaborating police force", in relation to a police collaboration agreement, means a police force (other than force 1) whose chief officer of police is a party to the agreement,

"England and Wales police force" means—

(a) any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London),

(b) the metropolitan police force, or

(c) the City of London police force,

"police collaboration agreement" has the same meaning as in section 78 (see subsection (6) of that section),

and references in this section to an England and Wales police force or a police force include the National Crime Agency (and references to the chief officer of police include the Director General of the National Crime Agency).

[Sections 81 to 83 unchanged]

84. Application of Part 3 to postal operators and postal services

(1) This Part applies to postal operators and postal services as it applies to telecommunications operators and telecommunications services.

(2) In its application by virtue of subsection (1), this Part has effect as if—

(a) any reference to a telecommunications operator were a reference to a postal operator,

(b) any reference to a telecommunications service were a reference to a postal service,

(c) any reference to a telecommunication system were a reference to a postal service,

(d) sections 61(3)(a) and 62 were omitted, […]

(da) the reference in sections 60A(8), 61(7A)(a) and 61A(8)(a) to events data were a reference to anything within paragraph (a) or (b) of the definition of "communications data" in section 262(3), and

(e) in Part 2 of Schedule 4, for "which is entity data" there were substituted "within paragraph (c) of the definition of "communications data" in section 262(3).

[Section 85 unchanged]

86. Part 3: interpretation

(1) In this Part—

"authorisation" means an authorisation under section 60A, 61 or 61A,

"designated senior officer"—

(a) […]

(b) in relation to any […] relevant public authority, has the meaning given by section 70(3),

"filtering arrangements" means any arrangements under section 67(1),

"officer", in relation to a relevant public authority, means a person holding an office, rank or position with that authority,

"relevant public authority" means a public authority which is a relevant public authority for the purposes of this Part by virtue of section 70(2) or 73(1).

(2) In this Part "local authority" means—

(a) a district or county council in England,

(b) a London borough council,

(c) the Common Council of the City of London in its capacity as a local authority,

(d) the Council of the Isles of Scilly,

(e) a county council or county borough council in Wales,

(f) a council constituted under section 2 of the Local Government etc (Scotland) Act 1994, and

(g) a district council in Northern Ireland.

(2A) In this Part, "serious crime" means, in addition to crime which falls within paragraph (a) or (b) of the definition of "serious crime" in section 263(1), crime where the offence, or one of the offences, which is or would be constituted by the conduct concerned is—

(a) an offence for which an individual who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) is capable of being sentenced to imprisonment for a term of 6 months or more (disregarding any enactment prohibiting or restricting the imprisonment of individuals who have no previous convictions), or

(b) an offence—

(i) by a person who is not an individual, or

(ii) which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.

(3) See also—

section 261 (telecommunications definitions),

section 262 (postal definitions),

section 263 (general definitions),

section 265 (index of defined expressions).

Part 4

Retention of Communications Data

General

87. Powers to require retention of certain data

(1) The Secretary of State may, by notice (a "retention notice") and subject as follows, require a telecommunications operator to retain relevant communications data if—

(a) the Secretary of State considers that the requirement is necessary and proportionate for one or more of the following purposes—

(i) in the interests of national security,

(ii) for the applicable crime purpose (see subsection (10A)),

(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,

(iv) in the interests of public safety,

(v) 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,

(vi) to assist investigations into alleged miscarriages of justice, and

(b) the decision to give the notice has been approved by a Judicial Commissioner.

(2) A retention notice may—

(a) relate to a particular operator or any description of operators,

(b) require the retention of all data or any description of data,

(c) identify the period or periods for which data is to be retained,

(d) contain other requirements, or restrictions, in relation to the retention of data,

(e) make different provision for different purposes,

(f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.

(3) A retention notice must not require any data to be retained for more than 12 months beginning with—

(a) in the case of communications data relating to a specific communication, the day of the communication concerned,

(b) in the case of entity data which does not fall within paragraph (a) above but does fall within paragraph (a)(i) of the definition of "communications data" in section 261(5), the day on which the entity concerned ceases to be associated with the telecommunications service concerned or (if earlier) the day on which the data is changed, and

(c) in any other case, the day on which the data is first held by the operator concerned.

(4) A retention notice must not require an operator who controls or provides a telecommunication system ("the system operator") to retain data which—

(a) relates to the use of a telecommunications service provided by another telecommunications operator in relation to that system,

(b) is (or is capable of being) processed by the system operator as a result of being comprised in, included as part of, attached to or logically associated with a communication transmitted by means of the system as a result of the use mentioned in paragraph (a),

(c) is not needed by the system operator for the functioning of the system in relation to that communication, and

(d) is not retained or used by the system operator for any other lawful purpose,

and which it is reasonably practicable to separate from other data which is subject to the notice.

(5) A retention notice which relates to data already in existence when the notice comes into force imposes a requirement to retain the data for only so much of a period of retention as occurs on or after the coming into force of the notice.

(6) A retention notice comes into force—

(a) when the notice is given to the operator (or description of operators) concerned, or

(b) (if later) at the time or times specified in the notice.

(7) A retention notice is given to an operator (or description of operators) by giving, or publishing, it in such manner as the Secretary of State considers appropriate for bringing it to the attention of the operator (or description of operators) to whom it relates.

(8) A retention notice must specify—

(a) the operator (or description of operators) to whom it relates,

(aa) each telecommunications service (or description of telecommunications service) to which it relates,

(b) the data which is to be retained,

(c) the period or periods for which the data is to be retained,

(d) any other requirements, or any restrictions, in relation to the retention of the data,

(e) the information required by section 249(7) (the level or levels of contribution in respect of costs incurred as a result of the notice).

(9) The requirements or restrictions mentioned in subsection (8)(d) may, in particular, include—

(a) a requirement to retain the data in such a way that it can be transmitted efficiently and effectively in response to requests,

(b) requirements or restrictions in relation to the obtaining (whether by collection, generation or otherwise), generation or processing of—

(i) data for retention, or

(ii) retained data.

(10) The fact that data which would be retained under a retention notice relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the requirement to retain the data is necessary for one or more of the purposes falling within sub-paragraphs (i) to (vi) of subsection (1)(a).

(10A) In this section, "the applicable crime purpose" means—

(a) to the extent that a retention notice relates to events data, the purpose of preventing or detecting serious crime;

(b) to the extent that a retention notice relates to entity data, the purpose of preventing or detecting crime or of preventing disorder.

(10B) In subsection (10A)(a), "serious crime" means, in addition to crime which falls within paragraph (a) or (b) of the definition of "serious crime" in section 263(1), crime where the offence, or one of the offences, which is or would be constituted by the conduct concerned is—

(a) an offence for which an individual who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) is capable of being sentenced to imprisonment for a term of 6 months or more (disregarding any previous enactment prohibiting or restricting the imprisonment of individuals who have no previous convictions), or

(b) an offence—

(i) by a person who is not an individual, or

(ii) which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.

(11) In this Part "relevant communications data" means communications data which may be used to identify, or assist in identifying, any of the following—

(a) the sender or recipient of a communication (whether or not a person),

(b) the time or duration of a communication,

(c) the type, method or pattern, or fact, of communication,

(d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted, or

(e) the location of any such system,

and this expression therefore includes, in particular, internet connection records.

Safeguards

88. Matters to be taken into account before giving retention notices

(1) Before giving a retention notice, the Secretary of State must, among other matters, take into account—

(a) the likely benefits of the notice, including in relation to one or more of the purposes mentioned in sub-paragraphs (i) to (vi) of section 87(1)(a) (purposes for which communications data may be retained),

(aa) the telecommunications services to which the retention notice relates,

(ab) the appropriateness of limiting the data to be retained by reference to—

(i) location, or

(ii) descriptions of persons to whom telecommunications services are provided,

(b) the likely number of users (if known) of any telecommunications service to which the notice relates,

(c) the technical feasibility of complying with the notice,

(d) the likely cost of complying with the notice, and

(e) any other effect of the notice on the telecommunications operator (or description of operators) to whom it relates.

(2) Before giving such a notice, the Secretary of State must take reasonable steps to consult any operator to whom it relates.

[Sections 89, 91 and 94 not reproduced due to minor amendments only; sections 90, 92, 93 and 95 unchanged]

96. Application of Part 4 to postal operators and postal services

(1) This Part applies to postal operators and postal services as it applies to telecommunications operators and telecommunications services.

(2) In its application by virtue of subsection (1), this Part has effect as if—

(a) any reference to a telecommunications operator were a reference to a postal operator,

(b) any reference to a telecommunications service were a reference to a postal service,

(c) any reference to a telecommunication system were a reference to a postal service,

(d) in section 87(3), for paragraph (b) there were substituted—

"(b) in the case of communications data which does not fall within paragraph (a) above but does fall within paragraph (c) of the definition of "communications data" in section 262(3), the day on which the person concerned leaves the postal service concerned or (if earlier) the day on which the data is changed,",

(e) for section 87(4) there were substituted—

"(4) A retention notice must not require an operator who provides a postal service ("the network operator") to retain data which—

(a) relates to the use of a postal service provided by another postal operator in relation to the postal service of the network operator,

(b) is (or is capable of being) processed by the network operator as a result of being comprised in, included as part of, attached to or logically associated with a communication transmitted by means of the postal service of the network operator as a result of the use mentioned in paragraph (a),

(c) is not needed by the network operator for the functioning of the network operator's postal service in relation to that communication, and

(d) is not retained or used by the network operator for any other lawful purpose,

and which it is reasonably practicable to separate from other data which is subject to the notice.", […]

(ea) the reference in section 87(10A)(a) to events data were a reference to anything within paragraph (a) or (b) of the definition of "communications data" in section 262(3),

(eb) the reference in section 87(10A)(b) to entity data were a reference to anything within paragraph (c) of the definition of "communications data" in section 262(3), and

(f) in section 87(11), the words from "and this expression" to the end were omitted.

[Sections 97 to 98 unchanged]

Part 8
Oversight Arrangements

Investigatory Powers Commissioner and other Judicial Commissioners

The Commissioners

227. Investigatory Powers Commissioner and other Judicial Commissioners

(1) The Prime Minister must appoint—

(a) the Investigatory Powers Commissioner, and

(b) such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners.

(2) A person is not to be appointed as the Investigatory Powers Commissioner or another Judicial Commissioner unless the person holds or has held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005).

(3) A person is not to be appointed as the Investigatory Powers Commissioner unless recommended jointly by—

(a) the Lord Chancellor,

(b) the Lord Chief Justice of England and Wales,

(c) the Lord President of the Court of Session, and

(d) the Lord Chief Justice of Northern Ireland.

(4) A person is not to be appointed as a Judicial Commissioner under subsection (1)(b) unless recommended jointly by—

(a) the Lord Chancellor,

(b) the Lord Chief Justice of England and Wales,

(c) the Lord President of the Court of Session,

(d) the Lord Chief Justice of Northern Ireland, and

(e) the Investigatory Powers Commissioner.

(5) Before appointing any person under subsection (1), the Prime Minister must consult the Scottish Ministers.

(6) The Prime Minister must have regard to a memorandum of understanding agreed between the Prime Minister and the Scottish Ministers when exercising functions under subsection (1) or (5).

(7) The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners.

(8) The Investigatory Powers Commissioner may, to such extent as the Investigatory Powers Commissioner may decide, delegate the exercise of functions of the Investigatory Powers Commissioner to any other Judicial Commissioner.

(9) Subsection (8) does not apply to the function of the Investigatory Powers Commissioner of making a recommendation under subsection (4)(e) or making an appointment under section 247(1).

(9A) Subsection (8) applies to the functions of the Investigatory Powers Commissioner under section 60A or 65(3B) only where the Investigatory Powers Commissioner is unable to exercise the functions because of illness or absence or for any other reason.

(10) The delegation under subsection (8) to any extent of functions by the Investigatory Powers Commissioner does not prevent the exercise of the functions to that extent by that Commissioner.

(11) Any function exercisable by a Judicial Commissioner or any description of Judicial Commissioners is exercisable by any of the Judicial Commissioners or (as the case may be) any of the Judicial Commissioners of that description.

(12) Subsection (11) does not apply to—

(a) any function conferred on the Investigatory Powers Commissioner by name (except so far as its exercise by any of the Judicial Commissioners or any description of Judicial Commissioners is permitted by a delegation under subsection (8)), or

(b) any function conferred on, or delegated under subsection (8) to, any other particular named Judicial Commissioner.

(13) References in any enactment—

(a) to a Judicial Commissioner are to be read as including the Investigatory Powers Commissioner, and

(b) to the Investigatory Powers Commissioner are to be read, so far as necessary for the purposes of subsection (8), as references to the Investigatory Powers Commissioner or any other Judicial Commissioner.

[Section 228 unchanged]

Main functions of Commissioners

229. Main oversight functions

(1) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to—

(a) the interception of communications,

(b) the acquisition or retention of communications data,

(c) the acquisition of secondary data or related systems data under Chapter 1 of Part 2 or Chapter 1 of Part 6, or

(d) equipment interference.

(2) Such statutory functions include, in particular, functions relating to the disclosure, retention or other use of—

(a) any content of communications intercepted by an interception authorised or required by a warrant under Chapter 1 of Part 2 or Chapter 1 of Part 6,

(b) acquired or retained communications data,

(c) data acquired as mentioned in subsection (1)(c), or

(d) communications, equipment data or other information acquired by means of equipment interference.

(3) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation)—

(a) the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service,

(b) the giving and operation of notices under section 252 (national security notices),

(c) the exercise of functions by virtue of section 80 of the Serious Crime Act 2015 (prevention or restriction of use of communication devices by prisoners etc),

(d) the exercise of functions by virtue of sections 1 to 4 of the Prisons (Interference with Wireless Telegraphy) Act 2012,

(e) the exercise of functions by virtue of Part 2 or 3 of the Regulation of Investigatory Powers Act 2000 (surveillance, covert human intelligence sources and investigation of electronic data protected by encryption etc),

(f) the adequacy of the arrangements by virtue of which the duties imposed by section 55 of that Act are sought to be discharged,

(g) the exercise of functions by virtue of the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11) (surveillance and covert human intelligence sources),

(h) the exercise of functions under Part 3 of the Police Act 1997 (authorisation of action in respect of property),

(i) the exercise by the Secretary of State of functions under sections 5 to 7 of the Intelligence Services Act 1994 (warrants for interference with wireless telegraphy, entry and interference with property etc), and

(j) the exercise by the Scottish Ministers (by virtue of provision made under section 63 of the Scotland Act 1998) of functions under sections 5 and 6(3) and (4) of the Act of 1994.

(4) But the Investigatory Powers Commissioner is not to keep under review—

(a) the exercise of any function of a relevant Minister to make subordinate legislation,

(b) the exercise of any function by a judicial authority,

(c) the exercise of any function by virtue of Part 3 of the Regulation of Investigatory Powers Act 2000 which is exercisable with the permission of a judicial authority,

(d) the exercise of any function which—

(i) is for the purpose of obtaining information or taking possession of any document or other property in connection with communications stored in or by a telecommunication system, or

(ii) is carried out in accordance with an order made by a judicial authority for that purpose,

and is not exercisable by virtue of this Act, the Regulation of Investigatory Powers Act 2000, the Regulation of Investigatory Powers (Scotland) Act 2000 or an enactment mentioned in subsection (3)(c), (h), (i) or (j) above,

(e) the exercise of any function where the conduct concerned is—

(i) conduct authorised by section 45, 47 or 50, or

(ii) conduct authorised by section 46 which is not conduct by or on behalf of an intercepting authority (within the meaning given by section 18(1)), or

(f) the exercise of any function which is subject to review by the Information Commissioner or the Investigatory Powers Commissioner for Northern Ireland.

(5) In keeping matters under review in accordance with this section, the Investigatory Powers Commissioner must, in particular, keep under review the operation of safeguards to protect privacy.

(6) In exercising functions under this Act, a Judicial Commissioner must not act in a way which the Commissioner considers to be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime, or

(c) the economic well-being of the United Kingdom.

(7) A Judicial Commissioner must, in particular, ensure that the Commissioner does not—

(a) jeopardise the success of an intelligence or security operation or a law enforcement operation,

(b) compromise the safety or security of those involved, or

(c) unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces.

(8) Subsections (6) and (7) do not apply in relation to any of the following functions of a Judicial Commissioner—

(a) deciding—

(i) whether to serve, vary or cancel a monetary penalty notice under section 7 or paragraph 16 of Schedule 1, a notice of intent under paragraph 4 of that Schedule or an information notice under Part 2 of that Schedule, or

(ii) the contents of any such notice,

(b) deciding whether to approve the issue, modification or renewal of a warrant,

(c) deciding whether to direct the destruction of material or how otherwise to deal with the situation where—

(i) a warrant issued, or modification made, for what was considered to be an urgent need is not approved, or

(ii) an item subject to legal privilege is retained, following its examination, for purposes other than the destruction of the item,

(d) deciding whether to—

(i) approve the grant, modification or renewal of an authorisation, or

(ii) quash or cancel an authorisation or renewal,

(e) deciding whether to approve—

(i) the giving or varying of a retention notice under Part 4 or a notice under section 252 or 254, or

(ii) the giving of a notice under section 90(10)(b) or 257(9)(b),

(f) participating in a review under section 90 or 256,

(g) deciding whether to approve an authorisation under section 219(3)(b),

(h) deciding whether to give approval under section 222(4),

(i) deciding whether to approve the giving or varying of a direction under section 225(3),

(j) making a decision under section 231(1),

(k) deciding whether to order the destruction of records under section 103 of the Police Act 1997, section 37 of the Regulation of Investigatory Powers Act 2000 or section 15 of the Regulation of Investigatory Powers (Scotland) Act 2000,

(l) deciding whether to make an order under section 103(6) of the Police Act 1997 (order enabling the taking of action to retrieve anything left on property in pursuance of an authorisation),

(m) deciding—

(i) an appeal against, or a review of, a decision by another Judicial Commissioner, and

(ii) any action to take as a result.

(8A) Subsections (6) and (7) also do not apply in relation to the functions of the Investigatory Powers Commissioner under section 60A or 65(3B).

(9) In this section—

"bulk personal dataset" is to be read in accordance with section 199,

"equipment data" has the same meaning as in Part 5 (see section 100),

"judicial authority" means a judge, court or tribunal or any person exercising the functions of a judge, court or tribunal (but does not include a Judicial Commissioner),

"police force" has the same meaning as in Part 2 (see section 60(1)),

"related systems data" has the meaning given by section 15(6),

"relevant Minister" means a Minister of the Crown or government department, the Scottish Ministers, the Welsh Ministers or a Northern Ireland department,

"secondary data" has the same meaning as in Part 2 (see section 16).

[Sections 230 to 237 unchanged]

Supplementary provision

238. Funding, staff and facilities etc

(1) There is to be paid to the Judicial Commissioners out of money provided by Parliament such remuneration and allowances as the Treasury may determine.

(2) The Secretary of State must, after consultation with the Investigatory Powers Commissioner and subject to the approval of the Treasury as to numbers of staff, provide the Judicial Commissioners with—

(a) such staff, and

(b) such accommodation, equipment and other facilities and services,

as the Secretary of State considers necessary for the carrying out of the Commissioners' functions.

(3) The Scottish Ministers may pay to the Judicial Commissioners such allowances as the Scottish Ministers consider appropriate in respect of the exercise by the Commissioners of functions which relate to the exercise by Scottish public authorities of devolved functions.

(4) In subsection (3)—

"devolved function" means a function that does not relate to reserved matters (within the meaning of the Scotland Act 1998), and

"Scottish public authority" has the same meaning as in the Scotland Act 1998.

(5) The Investigatory Powers Commissioner or any other Judicial Commissioner may, to such extent as the Commissioner concerned may decide, delegate the exercise of functions of that Commissioner to any member of staff of the Judicial Commissioners or any other person acting on behalf of the Commissioners.

(6) Subsection (5) does not apply to—

(a) the function of the Investigatory Powers Commissioner of making a recommendation under section 227(4)€ or making an appointment under section 247(1),

(b) any function which falls within section 229(8), or

(c) any function under section 58(4) or 133(3) of authorising a disclosure,

but, subject to this and the terms of the delegation, does include functions which have been delegated to a Judicial Commissioner by the Investigatory Powers Commissioner.

(7) The delegation under subsection (5) to any extent of functions by the Investigatory Powers Commissioner or any other Judicial Commissioner does not prevent the exercise of the functions to that extent by the Commissioner concerned.

[Sections 240 to 249 unchanged]

Schedule 4

Relevant Public Authorities and Designated Senior Officers etc

Section 70(1)

Part 1 Table of Authorities and Officers etc

Table

"(1) Relevant public authority	*(2) Paragraphs of section 60A(7) specified*	*(3) DSO: minimum office, rank or position*	*(4) Type of communications data that may be obtained by DSO*	*(5) Paragraphs of section 61(7) specified for DSO*	*(6) Paragraphs of section 61A(7) specified for DSO*
Police force maintained under section 2 of the Police Act 1996	60A(7)(a), (b), (c), (d), (e) and (g)	Inspector	Entity data	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
		Superintendent	All	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
Metropolitan police force	60A(7)(a), (b), (c), (d), (e) and (g)	Inspector	Entity data	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
		Superintendent	All	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
City of London police force	60A(7)(a), (b), (c), (d), (e) and (g)	Inspector	Entity data	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
		Superintendent	All	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
Police Service of Scotland	60A(7)(a), (b), (c), (d), (e) and (g)	Inspector	Entity data	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
		Superintendent	All	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
Police Service of Northern Ireland	60A(7)(a), (b), (c), (d), (e) and (g)	Inspector	Entity data	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
		Superintendent	All	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
British Transport Police Force	60A(7)(a), (b), (c), (d), (e) and (g)	Inspector	Entity data	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
		Superintendent	All	61(7)(a) and (c)	61A(7)(a), (b), (c) and (e)
Ministry of Defence Police	60A(7)(a), (b), (c), and (e)	Inspector	Entity data	61(7)(a) and (c)	61A(7)(a) and (c)
		Superintendent	All	61(7)(a) and (c)	61A(7)(a) and (c)
Royal Navy Police	60A(7)(a), (b), (c), and (e)	Lieutenant Commander	Entity data	61(7)(a) and (c)	61A(7)(a) and (c)
		Commander	All	61(7)(a) and (c)	61A(7)(a) and (c)
Royal Military Police	60A(7)(a), (b), (c), and (e)	Major	Entity data	61(7)(a) and (c)	61A(7)(a) and (c)

		Lieutenant Colonel	All	61(7)(a) and (c)	61A(7)(a) and (c)
Royal Air Force Police	60A(7)(a), (b), (c), and (e)	Squadron Leader	Entity data	61(7)(a) and (c)	61A(7)(a) and (c)
		Wing Commander	All	61(7)(a) and (c)	61A(7)(a) and (c)
Security Service	60A(7)(a), (b) and (c)	General Duties 4 or any other level 4 officer	Entity data	61(7)(a), (b) and (c)	
		General Duties 3 or any other level 3 officer	All	61(7)(a), (b) and (c)	
Secret Intelligence Service	60A(7)(a), (b) and (c)	Grade 6	All	61(7)(a), (b) and (c)	
GCHQ	60A(7)(a), (b) and (c)	GC8	All	61(7)(a), (b) and (c)	
Ministry of Defence	60A(7)(a) and (b)	Member of the Senior Civil Service or equivalent	All	61(7)(a)	
		Grade 7 in the Fraud Defence Unit	All		61A(7)(a)
Department of Health	60A(7)(b) and (d)	Grade 7 in the Medicines and Healthcare Products Regulatory Agency	All		61A(7)(a) and (b)
		Grade 7 in the Anti-Fraud Unit	All		61A(7)(a)
Home Office	60A(7)(b), (d) and (g)	Immigration inspector or equivalent with responsibility for investigations or other functions relating to immigration and border security	All		61A(7)(a)
		Immigration inspector or equivalent with responsibility for anti-corruption in relation to	All		61A(7)(a)

		investigations or other functions relating to immigration and border security Immigration inspector or equivalent with responsibility for asylum fraud investigations Immigration inspector or equivalent with responsibility for security and intelligence in the immigration detention estate	 All All		 61A(7)(a) 61A(7)(a), (b) and (e)
Ministry of Justice	60A(7)(b) and (d)	Manager in the security group of the National Offender Management Service responsible for intelligence Senior manager in the security group of the National Offender Manager Service responsible for intelligence	Entity data All		61A(7)(a) and (b) 61A(7)(a) and (b)
National Crime Agency	60A(7)(b), (e) and (g)	Grade 3 Grade 2	Entity data All		61A(7)(a), (c) and (e) 61A(7)(a), (c) and (e)
Her Majesty's Revenue and Customs	60A(7)(b)	Higher officer Senior officer	Entity data All		61A(7)(a) 61A(7)(a)
Department for Transport	60A(7)(b), (d) and (e)	Enforcement Officer in Maritime and Coastguard Agency Head of Enforcement in Maritime and	Entity data All		61A(7)(a) and (b) 61A(7)(a) and (b)

		Coastguard Agency Maritime Operations Commander (grade 7) in the Maritime and Coastguard Agency Principal Inspector in the Air Accident Investigation Branch, the Marine Accident Investigation Branch or the Rail Accident Investigation Branch	All All		61A(7)(c) 61A(7)(b)
Department for Work and Pensions	60A(7)(b)	Senior Executive Officer in Fraud and Error Services Senior Executive Officer in the Child Maintenance Group Central Legal Services	All All		61A(7)(a) 61A(7)(a)
An ambulance trust in England	60A(7)(e)	Duty Manager of Ambulance Trust Control Rooms	All		61A(7)(c)
Common Services Agency for the Scottish Health Service	60A(7)(b)	Head of Counter Fraud Services	All		61A(7)(a)
Competition and Markets Authority	60A(7)(b)	Member of the Senior Civil Service with responsibility for cartels or criminal enforcement	All		61A(7)(a)
Criminal Cases Review Commission	60A(7)(f)	Investigations Adviser	All		61A(7)(d)
Department for Communities in Northern Ireland	60A(7)(b)	Deputy Principal	All		61A(7)(a)
Department for the Economy in Northern Ireland	60A(7)(b)	Deputy chief inspector in trading standards services	All		61A(7)(a)
Department of Justice in Northern Ireland	60A(7)(b), (d) and (g)	Governor 4 in the Northern Ireland Prison Service	All		61A(7)(a), (b) and (e)

Financial Conduct Authority	60A(7)(b)	Head of department in the Enforcement and Market Oversight Division	All		61A(7)(a)
A fire and rescue authority under the Fire and Rescue Services Act 2004	60A(7)(e)	Watch Manager (Control)	All		61A(7)(c)
Food Standards Agency	60A(7)(b)	Grade 6	All		61A(7)(a)
Food Standards Scotland	60A(7)(b)	Head of the Scottish Food Crime and Incidents Unit	All		61A(7)(a)
Gambling Commission	60A(7)(b)	Senior manager	All		61A(7)(a)
Gangmasters and Labour Abuse Authority	60A(7)(b)	Head of operations	All		61A(7)(a)
Health and Safety Executive	60A(7)(b) and (d)	Band 1 inspector	All		61A(7)(a) and (b)
Independent Office for Police Conduct	60A(7)(b) and (g)	Director or an equivalent grade	All		61A(7)(a) and (e)
Information Commissioner	60A(7)(b)	Group manager Head of enforcement or an equivalent grade	Entity data All		61A(7)(a) 61A(7)(a)
National Health Service Business Services Authority	60A(7)(b)	Senior manager (of pay band 8b) in the Counter Fraud and Security Management Services Division	All		61A(7)(a)
Northern Ireland Ambulance Service Health and Social Care Trust	60A(7)(e)	Watch Manager (Control)	All		61A(7)(c)
Northern Ireland Fire and Rescue Service Board	60A(7)(e)	Watch Manager (Control)	All		61A(7)(c)
Northern Ireland Health and Social Care Regional Business Services Organisation	60A(7)(b)	Assistant Director Counter Fraud and Probity Services	All		61A(7)(a)
Office of Communications	60A(7)(b)	Senior associate	All		61A(7)(a)
Office of the Police Ombudsman for Northern Ireland	60A(7)(b)	Senior investigating officer	All		61A(7)(a)

Police Investigations and Review Commissioner	60A(7)(b) and (g)	Commissioner or Director of Operations	All		61A(7)(a) and (e)
Scottish Ambulance Service Board	60A(7)(e)	Watch Manager (Control)	All		61A(7)(c)
Scottish Criminal Cases Review Commission	60A(7)(f)	Investigations Adviser	All		61A(7)(d)
Serious Fraud Office	60A(7)(b)	Grade 6	All		61A(7)(a)
Welsh Ambulance Services National Health Service Trust	60A(7)(e)	Watch Manager (Control)	All		61A(7)(c)”

[Part 2 unchanged]