ANNEX:
OVERVIEW OF RELEVANT LEGISLATION

[This document has been agreed between the parties, subject to three "riders" by the Claimant, which are set out below where relevant]

Contents

1. This document presents an overview of the regime introduced by the Investigatory Powers Act 2016 (the "**Act**" or, where clarity requires, the "**2016 Act**"), and certain other relevant legislative provisions. It is intended to be an introduction to the structure and operation of the legislation. It does not refer to all of the relevant provisions for the purposes of the claim.

I) GENERAL PRIVACY PROTECTIONS – PART 1 OF THE ACT

2. The Act sets out "*the extent to which certain investigatory powers may be used to interfere with privacy*": s.1(1).

3. Part 1 of the Act contains both general "*duties in relation to privacy*" and other protections including offences and penalties: s.1(2)-(3).

4. S.2 of the Act contains "general duties" in relation to privacy in s 2(2). The duties apply where a public authority[1] is deciding whether to issue, renew or cancel a warrant under Parts 2, 5, 6 or 7 (as the Secretary of State may do: see below), to approve such a decision (as a Judicial Commissioner may do: see below), to grant, approve or cancel an authorisation under Part 3, or to give a notice under Part 4: s.2(1).

5. In exercising the specified functions, s.2(2) provides that 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 [2],*
> *(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*".

6. The 'have regard' duties in s.2(2) apply so far as is relevant in the particular context, and subject to the need to have regard to other considerations that are also relevant in that context: s.2(3). Section 2(4) provides that those other considerations may 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.*"

7. Part 1 of the Act also contains certain criminal offences, namely, intentional "unlawful interception" (s.3) and knowingly or recklessly "unlawfully obtaining communications data" (s.11).

8. *Unlawful interception* occurs where (a) a person intentionally intercepts[3] a communication in the course of its transmission by a public or private telecommunications system or a public postal service, (b) the interception is carried out in the UK and (c) the person lacks "*lawful authority*" to do so: s.3(1). So far as is material to the present claim, lawful authority will exist (inter alia) where the interception is carried out in accordance with a bulk interception warrant under Pt 6, Ch 1 of the Act: s.6(1)(a)(ii). The offence of unlawful interception is triable 'either way', and, on

[1] Defined as "*a public authority within the meaning of section 6 of the Human Rights Act 1998, other than a court or tribunal*": s.263(1).

[2] Section 2(5) gives certain examples of sensitive information for these purposes, including "*items subject to legal privilege*" and "*any information identifying or confirming a source of journalistic information*".

[3] Interception (etc.) for these purposes is defined in s.4 of the Act. In summary, it consists of doing a 'relevant act' in relation to a system (namely modifying or interfering with the system or its operation, monitoring transmissions made by means of the system, or monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system), whose effect is to make the content of any communication available to a person who is not the sender or intended recipient of the communication.

conviction on indictment, a person guilty of it is liable to up to 2 years' imprisonment or a fine (or both): s.3(6). Section 7 of the Act makes provision for the imposition of monetary penalties (of up to £50,000) by the Investigatory Powers Commissioner in cases of interception without lawful authority which do not, in the Commissioner's view, amount to the offence of unlawful interception, but this provision does not apply where a person was "*making an attempt to act in accordance with an interception warrant which might, in the opinion of the Commissioner, explain the interception*".

9. *Unlawfully obtaining communications data* occurs where, without lawful authority[4], a relevant person[5] knowingly or recklessly obtains communications data from a telecommunications operator or postal operator: s.11(1). It is a defence if the person can show that s/he acted in the reasonable belief that s/he had lawful authority to obtain the communications data. The offence of unlawfully obtaining communications data is also triable 'either way', and, on conviction on indictment, a person guilty of it is liable to up to 2 years' imprisonment or a fine (or both): s.11(4)(d).

II) BULK INTERCEPTION, ACQUISITION AND EQUIPMENT INTERFERNCE WARRANTS – PART 6

10. This claim concerns, inter alia, the 'bulk warrant' provisions in Part 6. In that regard:

    a. Pt 6 Ch 1 provides for bulk interception warrants.

    b. Pt 6 Ch 2 provides for bulk acquisition warrants (for communications data).

    c. Pt 6 Ch 3 provides for bulk equipment interference warrants.

11. The key provisions are set out below (bulk personal datasets, under Pt 7 of the Act, are considered separately).

(a) Bulk interception warrants (Pt 6 Ch 1)

12. A bulk interception must satisfy the following two cumulative conditions:

    a. Its "*main purpose*" is either the interception of "*overseas-related*" communications (i.e. communications sent or received by individuals who are outside the British Islands) or the obtaining of "*secondary data*" from such communications (s.136(2)); and

    b. The warrant authorises or requires its addressee to secure, by any conduct described in the warrant, one or more of (a) the interception, in the course of their transmission by means of a telecommunication system, of "*communications*" described in the warrant; (b) the obtaining of "*secondary data*" from such communications; (c) the "*selection for examination*", in any manner described in the warrant, of "*intercepted content*" or "*secondary data*" obtained

[4] S.81 makes provision for the circumstances in which conduct authorised by Pt 3 ('*Authorisations for obtaining communications data*') will be considered to be lawful.

[5] Defined in s.11(2) as a person who holds an office, rank or position with a relevant public authority (within the meaning of Part 3).

under the warrant; or (d) the "*disclosure*", in any manner described in the warrant, of anything obtained under the warrant to its addressee or any person acting on their behalf (s.136(4)).

13. A bulk interception warrant also authorises any conduct which it is necessary to undertake in order to do what is expressly authorised or required (s.136(5)).

14. "*Communication*" by s 261(1) relevantly includes "*anything comprising speech, music, sounds, visual images of data of any description*" and "*signals serving either for the impartation of anything*" between persons or things (or both) "*or for the actuation or control of any apparatus*". A communication may therefore be or contain "*content*" and/or "*secondary data*" (see immediately below).

15. "*Content*" by s 261(6) means relevantly "*any element of* [a] *communication, or any data attached to or logically associated with* [a] *communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but – (a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and (b) anything which is systems data is not content.*" (By s 157(1), "*intercepted content*" in relation to a bulk interception warrant means "*any content of communications intercepted by an interception authorised or required by the warrant*".)

16. "*Secondary data*" by s 137 means either of the following:

    a. First, "*systems data*" which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise) (s 137(4)). "*Systems data*" means "*any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of*" a postal service, a telecommunications system (including any apparatus that forms part of it), any telecommunications service provided by means of a telecommunication system, any system on which communications or other information are held (including any apparatus forming part of it) (a "*relevant system*"), and any service provided by means of a relevant system (s.263(4)–(5)).

    b. Secondly, "*identifying data*" that—(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 (s.137(5)). "*Identifying data*" means data which may be used to identify, or assist in identifying, any person, apparatus, system, service, event or the location of any person, event or thing (s.263(2)–(3)).

(b) Bulk acquisition warrants (Pt 6 Ch 2)

17. Bulk acquisition warrants authorise the obtaining, imposition of a requirement to obtain, "*selection for examination*" and disclosure of "*communications data*".

18. Specifically, a bulk acquisition warrant authorises or requires its addressee to secure, by any conduct described in the warrant, any one or more of (see s.158(5) and (6)):

    a. requiring a telecommunications operator specified in the warrant (i) to disclose to a person specified in the warrant any "*communications data*" which is specified in the warrant and is in the possession of the operator, (ii) to obtain any communications data specified in the warrant which is not in the operator's possession but which the operator is capable of obtaining, or (iii) to disclose to a person specified in the warrant any data so obtained;

    b. the selection for examination, in any manner described in the warrant, of communications data obtained under the warrant;

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

19. "*Communications data*" ("**CD**") is defined in s.261(5), as follows:

> "'*Communications data*', *in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data –*
> *(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and –*
> *(i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,*
> *(ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or*
> *(iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,*
> *(b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or*
> *(c) which –*
> *(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,*
> *(ii) is about the architecture of a telecommunication system, and*
> *(iii) is not about a specific person,*
> *but does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication.*"

20. Bulk acquisition warrants again authorise any conduct necessary to undertake what is expressly authorised or required and any conduct by a person required to assist giving effect to the warrant (s.158(7)).

(c) Bulk equipment interference warrants (Pt 6 Ch 3)

21. A bulk equipment interference warrant (s.176(1)):

    a. authorises or requires its addressee to "*secure interference with any equipment*" for the purpose of obtaining "*communication*", "*equipment data*" or "*any other information*"; and

    b. has as its "*main purpose*" to obtain "*overseas-related*" communications, information or equipment data.

22. In Pt 6 Ch 3:

    a. "*Communication*" again 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 or things (or both) or for the actuation or control of any apparatus (s.198(1)).

    b. "*Equipment*" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment (s.198(1)).

    c. "*Equipment data*" means either:

        i. "*Systems data*" (as defined in paragraph 16 above); or

        ii. "*Identifying data*" (as defined in paragraph 16 above) that is comprised in, part of, attached to or logically associated with, and is capable of being logically separated from, a communication or any other item of information without revealing anything of what might reasonably be considered to be the meaning of that communication / 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 (s.177(1)(b), (2)).

    d. "*Overseas-related information*" means information of individuals who are outside the British Islands (s.176(2)).

    e. "*Overseas-related communications*" are communications sent or received by individuals outside the British Islands (s.176(2)).

    f. "*Overseas-related equipment data*" means "*equipment data*" which (a) forms part of, or is connected with, overseas-related communications or overseas-related information, (b) would or may assist in establishing the existence of overseas-related communications or overseas-related information or in obtaining such communications or information, or (c) it would or may assist in developing capabilities in relation to obtaining overseas-related communications or overseas-related information (s.176(3)).

23. A bulk equipment interference warrant (s.176(4)):

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; and

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 so obtained; and/or

ii. the disclosure, in any manner described in the warrant, of any such material to the addressee or any person acting on their behalf.

24. Again, bulk equipment interference warrants authorise any conduct necessary to undertake what is expressly authorised or required and any conduct by a person required to assist giving effect to the warrant: s.176(5).

(d) **Criteria for approval of bulk intercept, acquisition and equipment interference warrants by the Secretary of State**

25. In the case of all three types of bulk warrant in Part 6, the power to issue a warrant resides with the Secretary of State, and is exercisable only following an application made by or on behalf of the head of an intelligence service (s.138(1), s.158(1) and s.178(1)).

26. In each case, the Secretary of State may only issue the warrant if s/he considers that:

a. the warrant is necessary in the interests of national security[6] or on that ground and for the purpose of preventing or detecting serious crime and/or in the interests of the economic well-being of the United Kingdom in so far as those interests are also relevant to the interests of national security[7]; and

b. the conduct authorised by the warrant is proportionate[8] to what is sought to be achieved by that conduct[9];

c. each of the specified "*operational purposes*" (see below) is a purpose for which the examination of material obtained under the warrant is or may be necessary, and the examination of material for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary[10];

[6] s.138(1)(b)(i), s.158(1)(a)(i), s.178(1)(b)(i).
[7] s.138(1)(b)(ii) and (2), s.158(1)(a)(ii) and (2), s.178(1)(b)(ii) and (2). A warrant may be considered necessary on the "economic well-being" ground only if the information / communications data which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands (s.138(3), s.158(3)) or if the interference with equipment which would be authorised by the warrant is considered necessary for the purposes of obtaining information relating to the acts or intentions of persons outside the British Island (s178(3)).
[8] The requirements of necessity and proportionality are addressed in Interception CoP, §§6.22-6.26; Bulk Acquisition CoP, §§4.6-4.11; Bulk EI CoP, §§6.15-6.19.
[9] s.138(1)(c), s.158(1)(b), s.178(1)(c).
[10] s.138(1)(d), s.158(1)(c), s.178(1)(d)

d. satisfactory arrangements made for the purposes of safeguards relating to disclosure etc. (see below) are in force in relation to the warrant[11];

e. the decision to issue the warrant has been approved by a Judicial Commissioner[12]. However, in relation to bulk equipment interference only, the requirement for prospective Judicial Commissioner approval does not apply where the Secretary of State considers that there is an urgent need to issue the warrant (see below for the provisions that require retrospective Judicial Commissioner approval in such cases).

27. In the case of bulk interception warrants and bulk equipment interference warrants only, the Secretary of State must additionally consider that:

a. in the case of bulk interception warrants, the main purpose of the warrant is the interception of overseas-related communications and/or the obtaining of secondary data from such communications (s138(1)(a)); and

b. in the case of bulk equipment interference warrants, the main purpose of the warrant is to obtain overseas-related communications, overseas-related information or overseas-related equipment data (s.178(1)(a)).

28. Detailed provision as to the format of, and the matters that must be included in, warrant applications under Part 6 Chs 1-3 of the Act appears at: §§6.17-6.20 of the Interception of Communications Code of Practice (the "**Interception CoP**") (bulk interception warrants); §§4.1-4.5 of the Bulk Acquisition of Communications Data Code of Practice (the "**Bulk Acquisition CoP**") (bulk acquisition warrants); and §§6.10-6.13 of the Equipment Interference CoP (the "**EI CoP**") (bulk equipment interference warrants).

29. In relation to all three types of bulk warrant, the decision to issue a warrant must be taken personally by the Secretary of State, and the warrant must be signed by the Secretary of State (s.141, s.160, s.182)[13].

30. Each of the three forms of bulk warrant under Pt 6 Chs 1-3 must, as issued, contain a provision stating that it is a bulk warrant of that kind and it must be addressed to the head of the intelligence service by whom or on whose behalf the warrant application was made; and it must describe the conduct that is authorised by the warrant (s.142(1)-(2), s.161(1)-(2), s.183(1)-(2)[14]). It must also specify the operational purposes for which any material obtained under the warrant may be selected for examination: see under "Operational Purposes" below.

(e) **Necessity and proportionality**

31. Warrants under Pts 6 Ch 1-3 of the Act may only be issued where the Secretary of State considers a warrant to be necessary for the specified statutory purposes (i.e. national

[11] s.138(1)(e), s.158(1)(d), s.178(1)(e)
[12] s.138(1)(g), s.158(1)(e), s.178(1)(f).
[13] Bulk equipment interference warrants may be signed by a designated senior official if it is not reasonably practicable for the warrant to be signed by the Secretary of State: ss.182(3)–(4) and EI CoP §§6.21-6.22.
[14] In the case of a bulk equipment interference warrant, the warrant must also "*describe the conduct that is authorised by the warrant*" (s.183(3)).

security, or national security *together with* the prevention / detection of serious crime or the interests of the economic well-being of the UK (so far as also relevant to the interests of national security), and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct, including whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means (see s.2(2)(a) of the Act, as referred to above).

(f) **Operational purposes**

32. The Secretary of State may not issue a bulk warrant under Pt 6 Ch 1, 2 or 3 unless s/he considers that (i) each of the "*specified operational purposes*" is a purpose for which the examination of material obtained under the warrant is or may be necessary, and (ii) the examination of material for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary: s.138(1)(d), s.158(1)(c), s.178(1)(d).

33. In that regard, a bulk warrant under each of Pt 6 Chs 1-3 must "*specify the operational purposes for which any [material] obtained under the warrant may be selected for examination*" (s.142(3), s.161(3), s.183(4)).

34. By ss.142(4)-(11), 161(4)-(11) and 183(5)-(12):

    a. The operational purposes specified in a warrant must be in a "*list of operational purposes*" maintained by the heads of the intelligence services as purposes which they consider are operational purposes for which material obtained under the type of bulk warrant may be selected for examination.

    b. An operational purpose may be specified in that list only with the approval of the Secretary of State, who may give such approval only if satisfied that the operational purpose is "*specified in a greater level of detail than*" "*national security*", "*preventing or detecting serious crime*" or "*the economic well-being of the United Kingdom so far as … relevant to the interest of national security*".

    c. The list of operational purposes must be provided by the Secretary of State to the Intelligence and Security Committee of Parliament every three months. The Prime Minister must review the list of operational purposes at least once a year.

    d. A warrant may specify all of the operational purposes which, at the time the warrant is issued, are specified in the list of operational purposes.

    e. The Codes of Practice indicate that the practice will (other than in exceptional circumstances) always be that *all* operational purposes (for the type of warrant) are included in every warrant: Interception CoP §6.67-6.68; Bulk Acquisition CoP §6.10; EI CoP §§6.6-6.7.

35. Interception CoP §§6.61-6.67 makes further provision relating to operational purposes.[15]

(g) **Existence of safeguards**

[15] And see Bulk Acquisition CoP §6.3 *et seq*, EI CoP §6.67 *et seq*.

36. Warrants in respect of the bulk powers in Pt 6 Chs 1–3 may only be issued if the Secretary of State considers that satisfactory "*safeguards*" are in place in respect of a number of matters: s.138(1)(e), s.158(1)(d), s.178(1)(e). Again, the relevant safeguards are largely the same in relation to each of the three key bulk powers.

(i) Safeguards relating to retention, copying and disclosure

37. In relation to every bulk (Pt 6) warrant, the Secretary of State must ensure that arrangements are in force for securing that:

    a. In relation to material obtained under the warrant, each of the following is limited to the minimum that is necessary for the "*authorised purposes*":

        i. the number of persons to whom any of the material is disclosed or otherwise made available;

        ii. the extent to which any of the material is disclosed or otherwise made available;

        iii. the extent to which any of the material is copied; and

        iv. the number of copies that are made;[16]

    and

    b. every "*copy*" made of any "*material*" obtained under a warrant is destroyed as soon as there are no longer any "*relevant grounds*" for retaining it[17];

    and

    c. specific safeguards relating to the examination of material are also in place[18] (see "Safeguards relating to selection for examination" below).

38. As to (a), the meaning of "*necessary for the authorised purposes*" is elucidated in the same terms for each of the three bulk powers: see s.150(3), s.171(3) and s.191(3)[19]. The

[16] See s.150(1)(a) and (2); s.171(1)(a) and (2); and s.191(1)(a) and (2).

[17] See s.150(1)(a) and (5); s.171(1)(a) and (5); and s.191(1)(a) and (5). There will no longer be 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 [national security together with one of the other specified grounds], and (b) its retention is not necessary for any of the purposes mentioned [in s.150(3)(b)-(e), s.171(3)(b)-(e) or s.191(3)(b)-(e) as the case may be]*": see s.150(1)(6), s.171(1)(6), s.191(1)(6). "Copy" has a statutory definition: see s.53(10) in relation to interception, s.191(9) in relation to material obtained under a bulk EI warrant, s.171(10) in relation to material obtained under a Bulk Acquisition warrant.

[18] See s.150(1)(b); s.171(1)(b); and s.191(1)(b)

[19] Specifically, "*something is necessary for the authorised purposes if, and only if –*
(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 138(2),
(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is or was addressed,
(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to this Act,
(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution, or

arrangements for ensuring that the requirements in s.150(2), s.171(2) and s.191(2) are met (i.e. that the various specified matters are kept to the minimum necessary for the authorised purpose) 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*": s.150(4), s.171(4) and s.191(4).

39. However, where material obtained under a warrant (or a copy) has been provided to any overseas authority, these safeguards do not apply: s.150(8), s.171(8) and s.191(8). Instead, the Secretary of State must ensure that requirements corresponding to those immediately above and immediately below apply "*to such extent (if any) as the Secretary of State considers appropriate*": see s.151(1) and (2)(a), s.171(9) and s.192(1)-(2).[20]

40. Pt 6 Ch 1 and Pt 6 Ch 3 contain statutory duties not to make "*unauthorised disclosures*" (s.156 and s.197), including disclosure of any material obtained under bulk interception or bulk equipment interference warrants, save where the disclosure is an "*excepted disclosure*" (including a disclosure authorised by the warrant, a disclosure to oversight bodies, etc.). It is a criminal offence to make an "*unauthorised disclosure*" of this kind[21]. Under Pt 6 Ch 2, s.174 makes it an offence for the telecommunications operator required to assist with the warrant (or a person employed or engaged for its business) to disclose the existence or contents of the warrant itself, but there is no offence of disclosing what is collected under a bulk acquisition warrant.

41. Each relevant CoP contains provisions addressing retention, copying and disclosure: Interception CoP §§9.15-9.31; Bulk Acquisition CoP §§9.4-9.13; EI CoP §§9.1-9.35.

(ii) Safeguards relating to selection for examination

42. The Act also requires the Secretary of State to ensure that safeguards relating to the examination of material are in force before issuing a bulk interception warrant, a bulk acquisition warrant or a bulk equipment interference warrant (ss.150(1)(b) and 152; ss.171(1)(b) and 172; and ss.191(1)(b) and 193)). Specifically, s/he must ensure that:

    a. The "*selection for examination*" of any material obtained under a warrant is carried out only in so far as is "*necessary for the operational purposes specified in the warrant*" at the time of the selection for examination (ss.152(1)(a), (2), 172(1)(a), (2)-(3) and 193(1)(a), (2)); and

---

(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."

[20] In the case of bulk interception warrants, the Secretary of State must additionally ensure 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*": s.151(1) and (2)(b). Under s.151(3), "*prohibited disclosure*" means a disclosure which, if made in the United Kingdom, would breach the prohibition in s.56(1) of the Act, which provides that no evidence may be adduced (etc.) in legal proceedings which either discloses, in circumstances from which its origin in 'interception-related' conduct may be inferred, any content of an interception communication or any secondary data obtained therefrom, or which tends to suggest that any interception-related conduct has or may have occurred or is going to occur. (Interception-related conduct is defined in s.56(2) and, read with s.156(1), covers matters such as the making of an application by any person for a warrant, or the issue of warrant, under Pt 6 Ch 1.) The prohibition in s.56(1) is subject to various exceptions set out in Schedule 3.

[21] See: ss.57-59 and 156 (bulk interception warrants); ss.132-134 and 197 (bulk interception warrants).

b. The selection of any of such material is "*necessary and proportionate in all the circumstances*" (ss.152(1)(b), 172(1)(b), 193(1)(b)).

43. Because an operational purpose may be included in a warrant for any of the purposes for which a warrant is issued, "*selection for examination*" may occur for "*operational purposes*" considered necessary for any of "*national security*", "*preventing or detecting serious crime*" or "*the economic well-being of the United Kingdom*" insofar as relevant to national security.

44. In relation to bulk interception warrants and bulk equipment interference warrants, the Secretary of State must also ensure that the selection for examination of respectively "*content*" and "*protected material*" meets any of the "*selection conditions*" (s.152(1)(c) and s.193(1)(c)) (the "**British Islands safeguard**".) The selection conditions are as follows (s.152(3) and s.193(3)):

a. Selection of the material for examination does not breach the prohibition on the use of selection criteria that are (i) referable to an individual known to be in the British Islands at that time and (ii) used for the purpose of identifying (a) the content of communications sent by or intended for that individual (for a bulk interception warrant) or (b) "*protected material*"[22] consisting of communications sent by, or intended for, that individual or "*private information*" relating to that individual (for bulk equipment interference warrants): ss.152(3)(a) and (4), 193(3)(a) and (4). Sections 152(4) and 193(4) respectively prohibit such selection for examination.

b. The warrant addressee "*considers*" (for a bulk interception warrant) or "*reasonably considers*" (for a bulk equipment interference warrant) that the selection for examination does breach that prohibition: ss.152(3)(b) and 193(3)(b));

c. The selection for examination of the "*content*" / "*protected material*" in breach of the prohibition is authorised by, respectively, s.152(5) or s.193(5), which authorise selection for examination where someone enters the British Islands or it becomes apparent that a belief that they were not in the British Islands was mistaken and a "*senior officer*" authorises continued selection for examination for up to five working days[23]; or

[22] Meaning any material obtained under the warrant other than material which is equipment data (see definition at §22.c above) or information (other than a communication or equipment data) which is not private information: s.193(9).

[23] These dis-apply the prohibition on selection for examination of material referable to a person known to be in the British Islands for the purpose of identifying their communications or where (a) criteria referable to an individual have been, or are being, used for the selection for examination of "*content*" / "*protected material*" in circumstances where the prohibition was not breached (or the addressee of the warrant considers it would not be breached, in the case of a bulk interception warrant, or reasonably considers it would not be breached, in the case of a bulk equipment interference warrant), (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 which would mean that the selection of the relevant content for examination would breach the prohibition, (c) since that time, a written authorisation to examine the relevant content using those criteria has been given by a senior officer, and (d) the selection of the relevant content for examination is made before the end of the "permitted period", being the fifth working day after the time at which the relevant change in circumstances appears to the addressee of the warrant: ss.152(5)(d) and (7); 193(5)(d) and (7)). "*Relevant change of circumstances*" means either that the individual concerned has entered the British Islands or that the addressee of the warrant was mistaken in believing that the individual was outside the British Islands: ss.152(6), 193(6).

d. Selection for examination of the "*content*" / "*protected material*" in breach of the prohibition is authorised by a targeted examination warrant issued under either Ch 1 Pt 2 or Pt 5.

Claimant's "rider":

(1) The British Islands safeguard in s 193(1)(c) for bulk interception warrants and bulk equipment interference warrants applies only to "*selection for examination*" of "*content*" (s 152(1)(c)) and "*protected material*" (s 193(1)(c)) respectively and not to other material obtained under a warrant. This is a central feature of this safeguard.

(2) There is no British Islands safeguard for bulk acquisition warrants under Pt 6 Ch 2.

45. The relevant Codes of Practice make further provision in relation to selection for examination: Interception CoP §6.71 *et seq*, Bulk Acquisition CoP §6.14 *et seq*; EI CoP §6.66 *et seq*.

(iii) Enhanced safeguards – special cases

Legally privileged material: bulk interception and bulk EI

46. **Basic position:** As to legally privileged material, the basic position for bulk interception and bulk equipment interference warrants is that:

a. Where "*intercepted content*" / "*protected information*" is selected for examination using criteria the (or a) purpose of which is, or use of which is likely, to identify legally privileged items, a senior official acting on behalf of the Secretary of State must approve the use of such criteria, having regard to "*the public interest in the confidentiality of the items subject to legal privilege*": ss.153(1)-(2), 194(1)-(2).

b. Approval may be given only if the official considers that there are specific arrangements in place for the handling, retention, use and destruction of items subject to legal privilege: ss. 153(4)(a), 194(4)(a).

c. In addition, where the (or a) purpose of using the criteria is to identify legally privileged items (but not otherwise, in particular not where the use of such criteria is likely to identify privileged items), approval may be given only if there are "*exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria*": ss.153(4), 194(4). An exhaustive definition of exceptional and compelling circumstances is set out in the Act (ss.153(5) and 194(5)).

47. **Communications furthering a criminal purpose:** Where the (or a) purpose of the use of criteria for selection for examination of "*intercepted content*" / "*protected information*" (but not other material obtained under a warrant) is to identify communications / information that would be subject to legal privilege if they were not made / created or held with the intention of furthering a criminal purpose, one of the "selection conditions" is met (see above) and the warrant addressee considers that the items are "*likely to be communications made with the intention of furthering a criminal purpose*", the

selection for examination may occur only if a "*senior official*" has approved the criteria: ss.153(6)-(7), 194(6)-(7). Approval may be given only if the official "*considers*" that the items "*are likely to be*" made / held or created "*with the intention of furthering a criminal purpose*": ss.153(8), 194(8).

48. **Where targeted examination warrants are required and the purpose is to select privileged items:** Where a targeted examination warrant is required in order to select for examination items subject to legal privilege[24] and the (or a) purpose is to authorise the selection for examination of items subject to legal privilege, s.27 and s.112 provide that: the warrant application must state that purpose; the person determining the application must have regard to the public interest in the confidentiality of items subject to legal privilege; and the person determining the application must issue a warrant only if s/he considers that (i) there are exceptional and compelling circumstances that make it necessary to select such items for examination and (ii) the relevant safeguards include specific arrangements for the handling, use, retention and destruction of such data (s.27(2)-(4), s.112(2)-(4)). The same definition of exceptional and compelling circumstances is used in s.27(6) and s.112(6).

49. **Retention following selection for examination:** Where an item subject to legal privilege is retained following its examination for a purpose other than its destruction, the addressee of the warrant must inform the Investigatory Powers Commissioner ("**IPC**") as soon as is reasonably practicable. The IPC must, unless he considers that the public interest in retaining the item outweighs the public interest in its confidentiality, and that retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury, direct that the item is destroyed or impose conditions as to the use/retention of the item: ss.153(9)-(12), 194(9)-(12).

Claimant's "rider":

The provisions in Pt 6 Ch 1 and Pt 6 Ch 3 that empower the IPC to give directions in relation to legally privileged material (ss 153(9)–(12) and 194(9)–(12)) do not prohibit the use of dissemination of the material before the IPC makes a determination. No equivalent provisions exist in Pt 6 Ch 2.

50. **Definition of "legal privilege":** "Items subject to legal privilege", in relation to England and Wales, has the same meaning as in s.10 Police and Criminal Evidence Act 1984; other definitions apply to Scotland and Northern Ireland: see s.263.

51. **CoP provision:** The safeguards applicable to the selection for examination of legally privileged material are explained at §9.48 *et seq* of the Interception CoP and §9.55 of the EI CoP. Among other matters, pursuant to the Interception CoP and Bulk EI CoP:

    a. Where an application for a targeted examination warrant is made where the (or a) purpose is to obtain items that would be subject to legal privilege, if they were not made with the intention of furthering a criminal purpose, the application must

[24] i.e. where the British Islands safeguard applies (and other "selection criteria" do not authorise selection for examination): see s.152(3)(d) (bulk interception), s.193(3)(d) (bulk equipment interference).

contain a statement to that effect and the reasons for believing that the criminal purpose exception applies: Interception CoP §9.57; Bulk EI CoP §9.53.

b. Wherever a person to whom a targeted examination warrant relates is a lawyer known to be acting in a professional capacity, or where communications are to be selected for examination using criteria referable to such a person, the authority must assume that the statutory protections for legally privileged material apply: Interception CoP §9.62; Bulk EI CoP §9.58.

c. In the event that privileged communications are inadvertently and unexpectedly selected for examination (so that the enhanced procedure has not been followed), any content so obtained must be handled strictly in accordance with ss.153/194, and the applicable provisions of the Codes, and no further privileged material may be intentionally selected for examination by reference to those criteria unless approved by a senior official: Interception CoP §9.61; EI CoP §9.57.

d. An authority will not act on or further disseminate legally privileged items without first informing the IPC that the items have been obtained or selected for examination, save where there is an urgent need to take action and it is not reasonably practicable to inform the IPC. In such cases, the agency should wherever possible consult a legal adviser. See Interception CoP §9.71; EI CoP §9.67.

Journalists: bulk interception and bulk EI

52. Relevant statutory safeguards apply to (i) "confidential journalistic material" (as defined in s.264[25]); and (ii) "sources of journalistic information" (as defined in s.263).

53. In relation to confidential journalistic material, where such material is retained following its examination for a purpose other than its destruction, the addressee of the warrant must inform the IPC as soon as is reasonably practicable: ss.154, 195.

Claimant's "rider":

The provisions in Pt 6 Ch 1 and Pt 6 Ch 3 that require reporting to the IPC where "*confidential journalistic material*" is retained (ss 154 and 195) do not prohibit the use of dissemination of the material before the IPC makes a determination. No equivalent provisions exist in Pt 6 Ch 2.

54. Additional statutory safeguards apply where a targeted examination warrant is required[26] and the (or a) purpose is the selection for examination of "*journalistic material*" which the authority believes is "*confidential journalistic material*". The warrant application must contain a statement that the purpose is to select such material for examination; and the person to whom the application is made may issue the warrant only if they consider that the arrangements under s.150 or s.191 (as the case may be) include specific arrangements for the handling, retention, use and destruction of communications containing confidential journalistic material: see s.28(2), s.113.

[25] S.264 contains statutory definitions of "*journalistic material*" and "*confidential journalistic material*".
[26] i.e. where the British Islands safeguard applies (and none of the other "*selection conditions*" is met).

55. The same applies, *mutatis mutandis,* where an application is made for a targeted examination warrant for the (or a) purpose of identifying a source of journalistic information i.e. the application must so state; and the person issuing the warrant must consider that appropriate arrangements are in place: s.29, s.114.

56. Under the Codes:

    a. Where an authorised person intends to select content or secondary data for examination in order to identify or confirm a source of journalistic information (and where it is not necessary to apply for a targeted examination warrant) s/he must notify a senior official[27] before so doing, and may not select the material for examination unless s/he has received the official's approval. The senior official may not provide such approval unless s/he considers that the agency has arrangements in place for the handling, retention, use and destruction of communications that identify sources of journalistic information. The same applies to the selection for examination of content in order to obtain confidential journalistic material. See Interception CoP §§9.84-9.86; Bulk EI CoP §§9.84-9.86.

    b. Where confidential journalistic material, or material identifying a journalistic source, is retained and disseminated to an outside body, reasonable steps should be taken to mark the disseminated information as confidential: Interception CoP §9.87; Bulk EI CoP, §9.80.

    c. The EI Code provides that where an application is made for a targeted examination warrant to identify a source, the "*public interest requiring such selection must override any other public interest*": EI Code, §9.76.

<u>Bulk Acquisition: lawyers and journalists</u>

57. The Bulk Acquisition CoP contains specific protections for the selection of data for examination in such cases:

    a. The Bulk Acquisition CoP requires officers to take into account any circumstances that might lead to an unusual degree of intrusion when selecting data for examination. Such circumstances are specifically stated to include "*all cases where it is intended or known that the data being selected for examination includes communications data of…lawyers, journalists…*": §6.23.

    b. Further provision is made as to journalists:

        i. The selection for examination of data in order to determine a source of journalistic information requires prior approval from a person holding the rank of Director or above, and any communications data so obtained and retained must be notified to the IPC at the next inspection: §6.28. This does <u>not</u> apply where the intent is to examine a journalist's communications data but not intended to determine the source of journalistic information: §6.30.

        ii. Further, where a journalist's data is selected, but the intention is not to determine a source of journalistic information, particular care must be taken

[27] As defined in s.145.

to ensure that the officer considers whether the intrusion is justified, giving proper consideration to the public interest, and whether there are alternative means for obtaining the information: §6.31.

(iv) Offences

58. The Act creates specific criminal offences that apply where a person deliberately selects material for examination that breaches the examination safeguards referred to above, knowing or believing that doing so will breach the safeguard: see ss.155, 173, 196. Such an offence is punishable on conviction on indictment by imprisonment for up to 2 years or an unlimited fine.

(h) **Requirement for independent approval of warrants by a Judicial Commissioner**

(i) General position (non-urgent warrants)

59. In the case of all three types of bulk warrant in Part 6, the Secretary of State's power to issue a warrant is subject to a requirement to obtain independent approval by a Judicial Commissioner (ss.140, 159, 179). The Judicial Commissioner is required to review the Secretary of State's conclusions as to:

    a. whether the warrant is necessary, by reference to the purpose for which the warrant is sought (e.g. national security);

    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 each of the specified operational purposes is a purpose for which the examination of the content/data obtained is or may be necessary;

    d. Whether the examination of content/data for each purpose is necessary on any of the grounds on which the Secretary of State considered the warrant to be necessary.

60. The Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review and must consider matters with a sufficient degree of care as to ensure that s/he complies with the general duties in relation to privacy imposed by s.2.

61. Where a Judicial Commissioner refuses to approve a decision to issue a warrant, s/he must give written reasons to the Secretary of State, and the Secretary of State may in that case ask the IPC (unless he was the Judicial Commissioner who gave the refusal) to decide whether to approve the decision to issue the warrant.

(ii) Judicial Commissioner approval of bulk equipment interference warrants in urgent cases

62. As set out above, in relation to bulk equipment interference warrants only, the Secretary of State is not required to obtain advance approval from a Judicial Commissioner in urgent cases: s.178(1)(f).

63. In such a case, the Secretary of State must inform a Judicial Commissioner that a warrant has been issued, following which that Judicial Commissioner must (before the end of the third working day after the day on which the warrant was issued) decide whether to approve the decision to issue the warrant, and notify the Secretary of State of that decision. If the Judicial Commissioner refuses to approve the decision, the warrant ceases to have effect (unless already cancelled) and may not be renewed: s.180. Where this occurs, 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: s.181(2). The Judicial Commissioner may (a) authorise further interference with equipment for the purpose of enabling the person to secure that anything in the process of being done under the warrant stops as soon as possible, (b) direct that any material obtained under the warrant is destroyed; and/or (c) impose conditions as to the use or retention of any of that material: s.181(3). In exercising these functions, the Judicial Commissioner may require an 'affected party' (being both the Secretary of State and the addressee of the warrant) to make representations, and must have regard to any representations made by an affected party (whether or not such representations were required): ss.181(4)-(5).

64. The Secretary of State may ask the IPC to review a decision made by any other Judicial Commissioner under s.181(3), whereupon the IPC may confirm the decision or make a fresh one: s.181(7).

65. Nothing in ss.180 or 181 affects the lawfulness of anything done under a warrant before it ceases to have effect, or anything being done under a warrant when it ceases to have affect before that thing could be stopped or that it is not reasonably practicable to stop: s.181(8).

(i) **Duration, modification and cancellation of bulk warrants**

66. As to duration, bulk interception warrants, bulk acquisition warrants and bulk equipment interference warrants (unless already cancelled) cease 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: ss.143, 162, 184(1) and (2)(b)[28].

67. As to renewal, the Secretary of State may renew a bulk interception warrant, bulk acquisition warrant or a bulk equipment interference warrant at any time during the period of 30 days ending with the day at the end of which the warrant concerned would otherwise cease to have effect, provided that certain "*renewal conditions*" are met. The relevant renewal conditions in each case are as follows:

> "*(a) that the Secretary of State considers that the warrant continues to be necessary –*
> *(i) in the interests of national security, or*
> *(ii) on that ground and on any other grounds falling within* section 138(2),

[28] Save that in relation to an 'urgent' bulk equipment interference warrant (i.e. one issued without advance Judicial Commissioner approval: see above), the warrant ceases to have effect at the end of the period ending with the fifth working day after the day on which the warrant was issued.

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

(c) that the Secretary of State considers that –

(i) each of the specified operational purposes (see section 142*) is a purpose for which the examination of intercepted content or secondary data obtained under the warrant continues to be, or may be, necessary, and*

(ii) the examination of intercepted content or secondary data for each such purpose continues to be necessary on any of the grounds on which the Secretary of State considers that the warrant continues to be necessary, and

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

(ss.144, 163 and 185 of the Act)

68. As to modification, the provisions of bulk interception warrants, bulk acquisition warrants and bulk equipment interference warrants may be modified at any time in order to add, vary or remove any specified operational purpose or to provide that the warrant no longer requires or authorises specified activities: ss.145, 164 and 186. The addition or variation of a specified operational purpose is designated as a "*major*" modification, which is subject to a separate requirement for Judicial Commissioner approval (except in urgent cases, where Judicial Commissioner approval of a major modification must be sought and obtained within three working days): ss.145(5), 146-147; ss.164(5), 165-166; ss.186(6), 187-188.

69. As to cancellation, the Secretary of State (or a senior official acting on his/her behalf) may cancel a bulk interception warrant, bulk acquisition warrant or bulk equipment interference warrant at any time. Moreover, s/he must cancel such a warrant where certain conditions are met, *viz.* that the warrant is no longer necessary in the interests of national security[29], the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct, or the examination of material obtained under the warrant is no longer necessary for any of the specified operational purposes (ss.148, 167, 189). Where a warrant is cancelled, the addressee of the warrant must, so far as reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible (ss.148(5), 167(5) 189(5)). A warrant that has been cancelled may not be renewed (ss.148(6), 167(6) and 189(6)).

III) TARGETED/THEMATIC EQUIPMENT INTERFERENCE WARRANTS UNDER PART 5

70. In addition to the bulk powers in Pt 6 Chs 1–3 of the Act, this claim concerns the lawfulness of aspects of the equipment interference regime in Part 5 of the Act.

[29] Save that this cancellation condition does not apply where the warrant has been modified so that it no longer authorises or requires: the interception of communications/obtaining of secondary data (in the case of a bulk interception warrant), the requiring of a telecommunications operator to disclose, or obtain and disclose, communications data specified in the warrant (in the case of a bulk acquisition warrant) or the securing of interference with any equipment or the obtaining of any communications, equipment data or other information (in the case of a bulk equipment interference warrant): ss.148(4), 167(4) and 189(4).

71. The only aspects presently in issue are the provisions described in the Act as "*targeted equipment interference warrants*" (being warrants which authorise or require the addressee to secure interference with any equipment for the purpose of obtaining communications, equipment data or any other information (s.99(2)) where the subject matter of warrant falls within s.101(1)(b)-(h) of the Act (commonly referred to as "*thematic equipment interference warrants*")[30]:

> "*…(b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;*
> *(c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;*
> *(d) equipment in a particular location;*
> *(e) equipment in more than one location, where the interference is for the purpose of a single investigation or operation;*
> *(f) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description;*
> *(g) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information;*
> *(h) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment*."

72. Several of the requirements for the issue of a targeted/thematic equipment interference warrant are similar to those that apply in relation to bulk warrants under Pt 6 Chs 1-3 (see above).

73. Thus, following an application made by an intelligence service, the Secretary of State may issue a targeted/thematic equipment interference warrant if:

    a. The Secretary of State considers that the warrant is necessary (i) in the interests of national security, (ii) for the purpose 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 (s.102(1)(a) and (5)). A targeted/thematic warrant may be issued for any of these purposes.

    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 (s.102(1)(b)).

    c. The Secretary of State considers that satisfactory safeguards are in force in relation to the warrant pursuant to ss.129 and 130 (s.102(1)(c)). Those safeguards (concerning retention and disclosure of material, and the disclosure of material to overseas authorities) are essentially equivalent to those that apply in relation to bulk warrants, save that, given the 'non-bulk' nature of the material obtained under targeted equipment interference warrants, there is no process of 'selection for examination' of material obtained pursuant to a

[30] At this stage, Liberty does not ask the Court to rule on the lawfulness of a targeted examination warrant whose subject matter is as specified in s.101(1)(a) of the Act, i.e. "*equipment belonging to, used by or in the possession of a particular person or organisation*".

targeted equipment interference warrant, and therefore no 'examination safeguards' applicable to that process.[31]

d. Except in urgent cases, the decision to issue the warrant has been approved by a Judicial Commissioner (s.102(1)(d)). The provisions for Judicial Commissioner approval, and for retrospective approval or refusal in urgent cases, in ss.108-110 match those in relation to bulk equipment interference warrants (see above).

74. Additional safeguards apply where the purpose of an equipment interference warrant is to obtain items subject to legal privilege: s.112 of the Act. These mirror the safeguards applicable to the selection for examination of material obtained under a bulk warrant (see e.g. s.153 in relation to bulk interception warrants).

75. Further, where an application is made for a targeted equipment interference warrant and the purpose, or one of the purposes of the warrant, is to obtain confidential journalistic material or to identify / confirm a source of journalistic information, the application must contain a statement to that effect and a warrant may be issued only if specific arrangements are in place for the handling, retention, use and destruction of communications or other items of information containing such material: ss.113 – 114.

76. In contrast to the bulk powers, Part 5 of the Act also makes provision for the issue of targeted equipment interference warrants by the Scottish Ministers (s.103), by the Secretary of State to the Chief of Defence Intelligence (s.104) and by certain "*law enforcement chiefs*" to appropriate law enforcement officers (s.106-107). The requirements for the issue of warrants in these instances are similar, but not identical, to the requirements in s.102 of the Act (issue of a targeted equipment interference warrant by the Secretary of State to the head of an intelligence service).

77. S.115 of the Act makes detailed provision for, inter alia, the details that must be included in a targeted equipment interference warrant, which depends on the subject matter of the warrant. For instance, where the subject matter of such a warrant is equipment belonging to (etc.) persons who form a group which shares a common purpose or carries on a particular activity, the warrant must contain a description of the purpose / activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe: s.115(3).

78. Sections 116-125 make detailed provision for the duration, renewal, modification and cancellation of warrants (including targeted equipment interference warrants) issued under Pt 5 of the Act.

IV) BULK PERSONAL DATASET WARRANTS – PART 7

79. Under s.199(1) of the Act, an intelligence service retains a bulk personal dataset ("**BPD**") where: (a) it 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

[31] As with the bulk powers, there are also enhanced safeguards in relation to the retention of legally privileged material obtained pursuant to a targeted equipment interference warrant (s.131 of the Act).

not, and are unlikely to become, of intelligence interest; (c) after any initial examination[32] of the content, the intelligence service retains the set of information for purpose of the exercise of its functions; and (d) the set is held, or to be held, electronically for analysis in the exercise of those functions.[33]

80. An intelligence service may not exercise a power to retain a BPD unless its retention is authorised by either a "*class BPD warrant*" (authorising an intelligence service to retain, or retain and examine, any BPD of a class described in the warrant) or a "*specific BPD warrant*" (authorising an intelligence service to retain, or retain and examine, any BPD described in the warrant): s.200.

81. Part 7 does not itself contain any power to obtain a BPD. Rather, the requirement for a BPD warrant concerns the retention and any subsequent examination of a BPD obtained by other means. Such means may include a warrant issued under s.5 of the Intelligence Services Act 1994 ("**ISA**"), other exercise of the intelligence services' "information gateway" powers under the ISA and Security Service Act 1989, and the other powers under the Act (except for Pt 6 Ch 2).

82. In the case of both a class BPD warrant and a specific BPD warrant, the decision to issue must be taken by the Secretary of State personally: s.211.

83. The requirement for the authorisation of retention of a BPD by way of a warrant under s.200 does not apply where an intelligence service exercises a power to retain or examine a BPD obtained under a warrant or other authorisation issued or given under the 2016 Act itself: s.201(1). However, as discussed below, the Secretary of State may direct that material so obtained should instead be treated as a BPD subject to the provisions of Pt 7.

(a) **Class BPD warrants**

84. On an application by the head of an intelligence service (or a person acting on his or her behalf), the Secretary of State may issue a class BPD warrant if (see s.204):

    a. The Secretary of State considers that the warrant is necessary (i) in the interests of national security, or (ii) for the purposes of preventing or detecting serious crime, or (iii) in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security (s.204(3)(a));

    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 (s.204(3)(b));

    c. Where the warrant authorises the examination of BPDs of the class described in the warrant, the Secretary of State considers that (i) each of the specified operational purposes is a purpose for which the examination of BPDs of that

[32] Section 220 provides for time limits on the initial examination of a set of information to determine whether it constitutes a BPD within the meaning of s.199 and, if so to seek a class or specific BPD warrant. Broadly speaking, the head of an intelligence service has 3 months to do so where the set of information was created in the UK, and 6 months where it was created outside the UK.

[33] "*Personal data*" means (a) data within the meaning of s.3(2) of the Data Protection Act 2018 (i.e. relating to an identified or identifiable living individual) which is subject to processing described in s.82(1) of that Act (processing by an intelligence service of personal data wholly or partly by automated means, etc.), or (b) data relating to a deceased individual which would fall within (a) if it related to a living individual.

class is or may be necessary, and (ii) the examination of BPDs 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 (s.204(3)(c)(i) and (ii)). S.212 makes further provision for the specification of operational purposes in a warrant, in terms which mirror the provisions of s.142 of the Act in relation to bulk interception warrants and the equivalent provisions relating to bulk acquisition warrants and bulk equipment interference warrants.

d. The Secretary of State considers that the arrangements made by the intelligence service for storing BPDs of the class to which the application relates and for protecting them from unauthorised disclosure are satisfactory (s.204(3)(d)).

e. The decision to issue the warrant has been approved by a Judicial Commissioner (s.204(3)(e)). See s.208 for the provision as to Judicial Commissioner approval.

85. A BPD may not, however, be retained, or retained and examined, pursuant to a class BPD warrant if the head of the intelligence service considers that the BPD consists of or includes, "*protected data*"[34] or "*health records*"[35] or that a substantial proportion of the BPD consists of "*sensitive personal data*"[36]: s.202(1) and (2).

86. Further, an intelligence service may not retain, or retain and examine, a BPD pursuant to a class BPD warrant if the head of the intelligence service considers that the nature of the BPD or the circumstances of its creation are such that its retention, or retention and examination, raises novel or contentious issues which ought to be considered by the Secretary of State and a Judicial Commissioner on an application for a specific BPD warrant.

(b) **Specific BPD warrants**

87. A specific BPD warrant may be sought by the head of an intelligence service (or a person acting on his or her behalf) where (see s.205(1)-(3)):

a. the BPD does not fall within a class described in a class BPD warrant; or

b. The BPD falls within a class described in a class BPD warrant but the intelligence service is prevented from retaining, or retaining and examining, it in reliance on the class BPD warrant by virtue of the restrictions in s.202 (see above) *or* that intelligence service at any time considers that it would be appropriate to seek a specific BPD warrant.

[34] Defined in s.203 as any data contained in a BPD other than systems data (see above), identifying data (see above) which is contained in the BPD which is capable of being logically separated from the BPD and if so separated would not reveal anything of what might reasonably be considered to be the meaning of the remaining data, and data which is not private information (which includes information relating to a person's private or family life).
[35] Defined in s.202(4) read with s.206(6) as a record, or copy of a record, which consists of information relating to the physical or mental health or condition of an individual, was made by or on behalf of a health professional in connection with that individual's care, and was obtained by the intelligence service from a health professional or a health service body (or from a person acting on their behalf).
[36] Meaning personal data consisting of information about an individual (whether living or deceased) or a kind mentioned in s.86(7)(a)-(e) of the Data Protection Act 2018 (covering matters such as personal data revealing political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation, and so on).

88. Subject to those points, the basic criteria for the issue of a specific BPD warrant by the Secretary of State are the same as those for the issue of a class BPD warrant, save that advance Judicial Commissioner approval need not be obtained in urgent cases: see s.205(6)(a)-(e). Provision for *post hoc* Judicial Commissioner approval of specific BPD warrants in urgent cases is made at ss.209 – 210 (in terms which mirror the provision for such approval in relation to bulk equipment interference warrants in urgent cases).

89. Additional safeguards apply to applications for specific BPD warrants in relation to:

    a. Health records: Section 206(1)-(3) provides that the Secretary of State may only issue a specific BPD warrant the purpose (or one of the purposes) of which is to authorise the retention, or retention and examination, of health records in "*exceptional and compelling circumstances*". Section 206(4)–(5) provides that, where the head of an intelligence services considers that a BPD includes or is "*likely*" to include health records (but it is not a or the purpose of a warrant to retain them), then the application must contain a statement to that effect.

    b. Protected data: Section 207 provides that, where the Secretary of State decides to issue a specific BPD warrant, s/he may impose conditions which must be satisfied before "*protected data*" (see s.203, considered at fn 34 above) retained in reliance on the warrant may be selected for examination on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection.

(c) **Duration, renewal, modification and cancellation of BPD warrants**

90. Sections 213-219 make provision for the duration, renewal, modification and cancellation of BPD warrants. The provision made largely mirrors the provision for the duration, etc., of bulk warrants under Pt 6 Chs 1-3 (including the requirement for Judicial Commissioner approval of "*major modifications*").

91. One different provision is s.219, which provides that, where a BPD warrant ceases to have effect because it expires without having been renewed or is cancelled:

    a. Within five working days after the expiry or cancellation of a BPD warrant, the head of the intelligence service to whom the warrant was addressed may either:

        i. apply for a specific or class BPD warrant authorising the retention, or retention and examination, of the whole or any part of the material previously retained pursuant to a BPD warrant (in which case the usual criteria for the grant of such an application will apply) (s.219(2)(a)); or

        ii. where the head of the intelligence service wishes to give further consideration to whether to apply for a further specific / class BPD warrant, apply to the Secretary of State for authorisation to retain / examine the whole or any part of the material retained in reliance on the warrant (s.219(2)(b)).

b. Where an application is made to the Secretary of State, s/he may direct that any of the material to which the application relates be destroyed (s.219(3)(a)), or (with the approval of a Judicial Commissioner) authorise the retention, or retention and examination, of any of that material, subject to such conditions as s/he considers appropriate, for a specified period not exceeding 3 months (s.219(3)(b)).

c. During that period, the head of an intelligence service may apply for a BPD warrant and must do so as soon as practicable and before the end of that period (s.219(7)).

d. S.219(8) provides that an intelligence service does not breach s.200 by virtue of its retention or examination of material to which a BPD warrant related where that intelligence service is seeking a further warrant or authorisation pursuant to s.219 during the periods mentioned above, as follows:

i. "*First period*": Five working days from when the BPD warrant cases to have effect;

ii. "*Second period*": The period beginning with the day of any application under s.219(2)(a) or (b) and ending with its determination;

iii. "*Third period*": The period during which retention or examination is authorised under s.219(3)(b) (at most three months);

iv. "*Fourth period*": Where an authorisation under s.219(3)(b) is given and the head of an intelligence service then makes an application under s.219(7) for a BPD warrant, the period beginning with the expiry of the authorisation under s.219(3)(b) and the determination of the application.

(d) **Safeguards relating to the examination of BPDs**

92. S.221 requires the Secretary of State to ensure that arrangements are in force for securing that:

a. any selection for examination of data contained in BPDs is carried out only so far as is necessary for the operational purposes specified in the warrant (at the time of the selection); and

b. the selection of any such data is necessary and proportionate in all the circumstances.

93. The Secretary of State must also ensure, in relation to every specific BPD warrant in which conditions in relation to the selection for examination of data under s.207 (see above) are imposed, that arrangements are in force for securing that any selection for examination of protected data on the basis of criteria referable to an individual known to be in the British Islands at the time of the selection is in accordance with the conditions specified in the warrant.

94. As with the bulk powers in Pt 6 Chs 1-3, enhanced safeguards apply to the selection for examination pursuant to a specific BPD warrant of items subject to legal privilege (which differ depending on whether it is the / a purpose of the warrant to obtain privileged items, this is likely, or the addressee of a warrant considers that the data is not privileged because it or any underlying material is likely to be data or underlying material created or held with the intention of furthering a criminal purpose): s.222.

95. It is a criminal offence, punishable on conviction on indictment by a prison term of up to 2 years or an unlimited fine, to deliberately select data for examination under a class BPD warrant or a specific BPD warrant, knowing or believing that the selection of that data is in breach of certain specified safeguards (e.g. that any such selection is carried out only so far as is necessary for the operational purposes specified in the warrant, and so on): s.224.

(e) Application of Pt 7 to BPDs obtained under other powers in the Act

96. Section 225 provides that the Secretary of State may, on an application by the head of the intelligence service, give a direction that the intelligence service may retain, or retain and examine, a BPD that has been obtained under a warrant issued under another provision of the Act (except a bulk acquisition warrant under Pt 6 Ch 2). In such a case, the power under which the BPD was obtained ceases to apply, and the intelligence service thereafter requires the authorisation of either a class BPD warrant or a specific BPD warrant. Such a direction may provide for any "*associated regulatory provision*" specified in the direction to continue to apply in relation to the BPD (meaning any provision which is made by or for the purposes of the Act (other than Pt 7) that applied immediately prior to the direction). A direction under s.225 may only be given with the approval of a Judicial Commissioner, and it may not be revoked (it may be varied, but only for the purpose of altering or removing any provision included in the direction).

V) ACQUISITION AND RETENTION OF COMMUNICATIONS DATA – PTS 3 AND 4 OF THE ACT

97. Parts 3 and 4 of the Act were the subject matter of the February 2018 hearing. However, certain amendments to those Parts of the Act have taken effect since the Court gave its judgment in these proceedings on 27 April 2018.

98. Part 4 relates to the procedure for requiring telecommunications providers to *retain* communications data and Part 3 relates to the procedure for authorisation for relevant public authorities to *obtain* communications data. Those Parts of the Act are supplemented by the Communications Data Code of Practice (November 2018) (the "**CD CoP**"), which provides guidance on the procedures to be followed when acquisition of communications data takes place under Part 3 and when communications data is retained under Part 4.

(a) Retention of communications data – Part 4

99. Section 87 provides that the Secretary of State may, by notice (a "*retention notice*") 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 specified purposes and (b) the decision to give the notice has been approved by a Judicial Commissioner.

100. Since the Court's judgment in February 2018, the specified purposes (in s.87(1)) have been amended[37]. They are now restricted to retention that is necessary and proportionate: (i) in the interests of national security, (ii) for the applicable crime purpose (see s.87(10A)), 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, and (vi) to assist investigations into alleged miscarriages of justice. The crime purpose for which events data (such as call histories and location information) can be retained and acquired is restricted to 'serious crime', whereas entity data (such as the name of a subscriber to a service) can be obtained in relation to the full range of crimes. The provisions requiring approval of retention notices by a Judicial Commissioner have now come into force.[38]

101. As the Court noted in paragraphs [129] to [138] of its 27 April 2018 judgment:

    a. s.87(2) provides, *inter alia*, that a notice may relate to a "description of data", may relate to a particular operator or to a description of operators, and that a retention notice may specify the period of time for which data is to be retained, which may not exceed 12 months;

    b. before the Secretary of State may serve a retention notice, s/he must have regard to, among other matters, the factors listed in s.88(1), which comprise the likely benefits of serving the notice, the number of users to which the notice relates, the technical feasibility and costs of complying with the notice and any other effect on the telecommunications operator to be served;

    c. a retention notice may not be given unless the Secretary of State's decision has been approved by a Judicial Commissioner under s.89, requiring a review of whether the requirements in the proposed notice are necessary and proportionate, applying the same principles as would be applied in judicial review, and ensuring that his or her consideration is sufficiently careful so as to comply with the duties in s.2 of the Act;

    d. a telecommunications operator which receives a retention notice may refer the notice back to the Secretary of State for a formal process of review, in accordance with ss.90 to 91. These provisions are now fully in force and require the Secretary of State to consult and take into account the report of a Technical Advisory Board and a Judicial Commissioner (s.90(6), (9) and (10)). The Secretary of State may not vary or confirm a notice (as opposed to revoking a notice) unless that decision is approved by the IPC (s.90(11)).

[37] By the Data Retention and Acquisition Regulations 2018 (SI 2018/1123, 1 November 2018).
[38] Pursuant to reg. 4(a) of the Investigatory Powers Act 2016 (Commencement No. 7 and Transitional and Saving Provisions) Regulations 2018/873

(b) **Acquisition of communications data – Part 3**

102. Applications to *acquire* communications data can be authorised by three separate categories of individual, depending on the circumstances:

a. s.60A of the Act confers power on the IPC to authorise applications for communications data in relation to the purposes set out in s.60A(7), i.e: (a) national security; (b) the applicable crime purpose (see s.60A(8)); (c) the economic well-being of the United Kingdom so far as relevant to the interests of national security; (d) public safety; (e) preventing death or injury or any damage to physical or mental health, or mitigating any injury or damage to physical or mental health; (f) assisting investigations into alleged miscarriages of justice, or (g) identifying dead or incapacitated persons;

b. s.61 provides for the authorisation of communications data requests relating to national security. Where an application for communications data is for the purpose of national security under s.61(7)(a), or economic well-being where relevant to national security under s.61(7)(c), or where it is an application made by a member of an intelligence agency under s.61(7)(b) (the applicable crime purpose), an application may, as an alternative to IPC authorisation under s.60A, be authorised internally by a designated senior officer in the public authority. The designated senior officer must, except where provided for in the Act, be independent of the operation concerned (see s.63(1));

c. s.61A provides for designated senior officers to grant authorisations in urgent cases. Examples of urgent circumstances, including an immediate threat of loss or serious harm to human life, an urgent operational requirement for data that will directly assist the prevention or detection of the commission of a serious crime or a credible and immediate threat to national security, are set out in CD CoP §5.31.

103. Under s.60A(1), the IPC may grant an authorisation, on an application made by a relevant public authority, where he considers that: (a) it is *necessary* for the relevant public authority to obtain communications data for a specified purpose falling within subsection 60A(7); (b) 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.

104. Similar conditions of necessity and proportionality apply for authorisations under s.61 and 61A (with the additional requirement of urgency in s.61A).

105. Ss.62-66 have been moved and grouped together under a new heading "*Further provision about authorisations*". They impose additional restrictions on acquisition of communications data, including:

a. Preventing local authorities from acquiring internet connection records for any purpose, and restricting the ability of other public authorities to access internet connection records to specific circumstances and purposes. This imposes a requirement for additional consideration of the proportionality of the

application in relation to the level of processing and disclosure involved (see s.62 and CD CoP, Part 9);

b. Restricting the ability of designated senior officers to grant an authorisation if the officer is working on the relevant investigation or operation (s.63);

c. Specifying the content of authorisations (s.64);

d. Limiting the duration of authorisations (to one month, or 3 days in the case of urgent authorisations), subject to renewal or cancellation (s.65); and

e. Imposing duties on telecommunications providers, including a duty to obtain or disclose the data in a way that minimises the amount of data that needs to be processed for the purpose concerned (s.66).

106. Further safeguards are put in places by ss.76 and 77, in particular:

a. A requirement (subject to certain exceptions) to consult a person who is acting as a single point of contact in relation to the making of applications, before making any application to IPCO for authorisation under s.60A, or before a designated senior officer grants authorisation under s.61 or s.61A. Such consultation may encompass questions relating to the most appropriate methods for obtaining data, any unintended consequences of the proposed authorisation, and any issues as to the lawfulness of the proposed authorisation; and

b. A requirement for Judicial Commissioner approval for authorisations under s.61 or s.61A (or delegated decisions made under s.60A) to identify or confirm journalistic sources, where the authorisation is not necessary because of an imminent threat to life. S.77(6) requires, in particular, that the Judicial Commissioner must 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. This provision is supplemented by the CD CoP, §§8.23ff.

(c) RIPA Part 1 Chapter 2

107. The regime for the acquisition of communications data under Regulation of Investigatory Powers Act 2000 Pt 1 Ch 2 has not yet been repealed. It operates alongside IPA Pts 3–4 for some public authorities. The provisions have been amended to provide that "*traffic data*" and data about the use of any postal service, telecommunication service or part of a telecommunication system (see s.21(4)(a)-(b)) can only be acquired in relation to "*serious crime*".

VI) OVERSIGHT ARRANGEMENTS – PART 8 OF THE ACT

108. Part 8 makes provision for a series of oversight arrangements in relation to the exercise of the range of investigatory powers under the Act. In particular, Part 8:

a. provides for the appointment of a new IPC (the Investigatory Powers Commissioner) and other Judicial Commissioners; and

b. provides for the jurisdiction of the (existing) Investigatory Powers Tribunal ("**IPT**") in respect of the use of investigatory powers under the Act and introduces a new right of appeal against the IPT's decisions.

(a) **The IPC and the Judicial Commissioners**

109. The IPC replaces and consolidates the functions of a series of pre-existing oversight bodies, all of which were all abolished by the Act: s.240.

110. Section 227(1) requires the Prime Minister to appoint the IPC and such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the Judicial Commissioners' functions. The IPC and the Judicial Commissioners must hold or have held a high judicial office: s.227(2). The current (and first) IPC is the Rt Hon Lord Justice Fulford (appointed February 2017). His Deputy is the Rt Hon Sir John Goldring. The IPC is supported in his role by the Office of the Investigatory Powers Commissioner ("**IPCO**"). S.238 of the Act makes general provision for funding, staff and facilities in relation to the IPC and the Judicial Commissioners.

111. The IPC's main oversight functions are set out in s.229, and include (so far as is material):

a. keeping under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to *inter alia* the interception of communications, the acquisition and retention of communications data and equipment interference: s.229(1)-(2);

b. keeping under review (including by way of audit, inspection and investigation) the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service: s.229(3)(a);

c. keeping under review the operation of safeguards to protect privacy: s.229(5).

(i) Error reporting and notification to victims

112. Under s. 235(6) a public authority, telecommunications operator or postal operator must report to the IPC any "*relevant error*" (as defined in s. 231(9)). A "*relevant error*" means an error (a) by a public authority in complying with any requirements which are imposed on it by virtue of the Act or any other enactment and which are subject to review by a Judicial Commissioner and (b) of a description identified for this purpose in a code of practice specified under Schedule 7: s.231(9). The IPC must also keep under review the definition of "*relevant error*": s.231(9).

113. Under the Interception CoP §10.17, EI CoP §10.19, Bulk Acquisition CoP §10.15 and BPD CoP §8.11, relevant errors must be notified to the IPC "*as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance processes that a relevant error has occurred*". Under CD CoP §24.26, the requirement is to report the error to the authority's senior responsible officer and then to the IPC "*within no more than five working days of it being established that an error has occurred*".

114. Under s.231(1) of the Act, the IPC must[39] 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[40]. The IPC may not decide that an error is serious unless he considers that the error has caused significant prejudice or harm to the person concerned: s.231(2). The fact that there has been a breach of a person's Convention rights is not sufficient by itself to amount to a serious error: s.231(3).

115. When informing someone of an error, the IPC must also (s.231(6)):

> *"(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)."*

(ii) Annual reporting by the IPC

116. The IPC must also, 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 (s.234(1)), including the detailed matters specified in s.234(2), which include statistics on the use of investigatory powers, information about the results and impact of such use, information about the operation of the safeguards under the Act, and so on. A report under s.234(1) must also include information about the number of relevant errors of which the IPC has become aware during the year to which the report relates, the number of such errors which the IPC has decided were serious errors, and the number of persons who have been informed of such errors: s.231(8).

117. On receipt of a report from the IPC under s.234(1), the Prime Minister must publish the report and lay a copy before Parliament: s.234(6)[41]. The IPC also has a discretion, where he considers it appropriate, to make a report to the Prime Minister on any matter relating to the functions of the Judicial Commissioners: s.234(4). A report under s.234(1) or (4) may, in particular, include such recommendations as the IPC considers appropriate about any matter relating to the functions of the Judicial Commissioners. The IPC is also required to make any report to the Prime Minister which the Prime Minister has requested: s.234(3).

(iii) Judicial Commissioners' functions

118. The main relevant functions of Judicial Commissioners under the Act concern the giving of authorisations for warrants and notices issued by the Secretary of State in respect of

---

[39] Having first given the public authority which has made the error the opportunity to make submissions: s.231(5).
[40] In deciding this, the IPC must consider, in particular "*(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*".
[41] S.231(7) provides that, on consultation with the IPC, the Prime Minister may exclude from the published version of the report any part of the report that would be contrary to the public interest or prejudicial to national security or other matters specified in s.231(7)(a)-(d).

the exercise of the various investigatory powers in the Act: see above. However, they also have a number of more general duties and powers under Part 8 of the Act.

119. Under s.229(6)-(7), when exercising functions under the Act, a Judicial Commissioner must not act in a way that s/he considers to be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime or the economic well-being of the United Kingdom, and must in particular ensure that the Commissioner does not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, or unduly impede the operational effectiveness of an intelligence service, police force, government department or Her Majesty's forces. However, these general duties do not apply in relation to certain of the Judicial Commissioners' functions, including deciding whether to approve the issue, modification or renewal of a warrant (s.229(8)(b)) and deciding whether to approve the grant, modification or renewal of a retention notice (s.229(8)(e)(i)).

120. Under s.235, the Judicial Commissioners have powers in relation to the carrying out of investigations, inspections and audits, including a power to obtain documents and information and to require assistance (including access to apparatus, systems, facilities and services) from "*relevant persons*", including any person who holds (or has held) an office, rank or position with a public authority and any telecommunications or postal operator who is, has been or may become subject to a requirement imposed by virtue of the Act (s.235(7)).

(b) **The IPT**

121. The Tribunal was established by s.65(1) of the Regulation of Investigatory Powers Act 2000 ("**RIPA**"). Members of the Tribunal must either hold or have held high judicial office or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).

122. The Tribunal has exclusive jurisdiction to consider claims under s.7(1)(a) of the HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss.65(2)(a), 65(3)(a) and 65(3)(b) of RIPA).

123. The Tribunal may also consider and determine any complaints by a person who is aggrieved by certain conduct[42] which s/he believes to have taken place (in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system, and to have taken place in "*challengeable circumstances*" or to have been carried out by or on behalf of the intelligence services (ss.65(2)(b), 65(4) of RIPA). Conduct takes place in "*challengeable circumstances*" when either it is the conduct of a public authority and it takes place with the (purported) authority of (inter alia) a warrant under Pts 5, 6 or 7 of the 2016 Act, an authorisation or notice under Pt 3 of the 2016 Act, or a retention notice under Pt 4 of the 2016 Act, *or* the circumstances are such that it would not have been appropriate for the

[42] A wide range of such conduct is specified in s.65(5) RIPA, and it includes the full panoply of actions that may be taken under the impugned parts of the 2016 Act.

conduct to take place without at least proper consideration having been given to whether such authority should be sought (RIPA, ss.65(7) and (8)).

124. Any person, regardless of nationality, may bring a complaint to the Tribunal. The IPT considered the scope of its jurisdiction and the extent of the knowledge or evidence of the use of investigatory powers required to make a claim in *Human Rights Watch v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib_15_165-CH.

125. Complaints are investigated and then determined by the Tribunal "*by applying the same principles as would be applied by a court on an application for judicial review*" (s.67(3) of RIPA). S.68(6) of RIPA gives the Tribunal powers to order production of materials by, among others, every person holding office under the Crown. Further, under s.232(1) of the 2016 Act, a Judicial Commissioner must give the IPT all such documents, information and other assistance as the IPT may require in connection with the investigation, consideration or determination of any matter.

126. Subject to any provision in its rules, the Tribunal may — at the conclusion of a claim — make any such award of compensation or other order as it thinks fit, including, but not limited to, an order quashing or cancelling warrants, authorisations, notices and directions given under the 2016 Act and an order requiring the destruction of any records of information which have been obtained in exercise of any power conferred by a warrant, authorisation or notice under the Act, or which are held by any public authority in relation to any person: s.67(7) of RIPA.

127. S.242 of the 2016 Act introduced a new s.67A of RIPA, which provided (for the first time) for a right of appeal on a point of law from final decisions of the IPT which are not procedural to the Court of Appeal. A decision of the Tribunal is subject to judicial review: *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22.