## APPENDIX B: THE BPD REGIME

1. The regime in respect of Bulk Personal Datasets ("BPD") which is relevant to the activities of the Intelligence Services principally derives from the following statutes:

   (a) the Security Services Act 1989 ("the SSA") [**Auths/tab 3**] and the Intelligence Services Act 1994 ("the ISA") [**Auths/tab 4**];

   (b) the Counter-Terrorism Act 2008 ("the CTA") [**Auths/tab 9**];

   (c) the Human Rights Act 1998 ("the HRA") [**Auths/tab 6**];

   (d) the Data Protection Act 1998 ("the DPA") [**Auths/tab 5**]; and

   (e) the Official Secrets Act 1989 ("the OSA") [**Auths/tab 2**].

   These are addressed at **pages 1-6** below.

2. There are also important **oversight mechanisms** in the regime provided by the Interception of Communications Commissioner, the Intelligence Services Commissioner, the Intelligence and Security Committee and the Tribunal (see **pages 7-12** below).

3. In addition,

   (a) Where BPDs have been obtained by means of RIPA/ISA powers, the relevant **Codes of Practice** have been applied (see **pages 13-14** below); and

   (b) GCHQ, MI5 and SIS have a number of **internal arrangements** in relation to BPD (see **pages 15-44** below).

**The SSA and ISA**

*Security Service functions*

4. By s.1(2) to (4) of the Security Service Act 1989 ("SSA") [**Auths/tab 3**], the functions of the Security Service are the following:

   *"the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means."*

   *"to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands."*

   *"to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime."*

5. The Security Service's operations are under the control of a Director-General who is appointed by the Secretary of State (s.2(1)). By s.2(2)(a) it is the Director-General's

duty to ensure:

*"…that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings;…"*

***SIS functions***

6. By s.1(1) of the ISA [**Auths/tab 4**], the functions of SIS are:

*"(a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and*
*(b) to perform other tasks relating to the actions or intentions of such persons."*

7. By s.1(2) those functions are *"exercisable only-*

*"(a) in the interests of national security, with particular reference to the defence and foreign polices of Her Majesty's Government in the United Kingdom; or*

*(b) in the interests of the economic well-being of the United Kingdom; or*

*(c) in support of the prevention or detection of serious crime."*

8. SIS's operations are under the control of a Chief, who is appointed by the Secretary of State (s.2(1)). The Chief of SIS has a duty under s.2(2)(a) of the ISA to ensure:

*"(a) that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary-*

*(i) for that purpose;*

*(ii) in the interests of national security;*

*(iii) for the purpose of the prevention or detection of serious crime; or*

*(iv) for the purpose of any criminal proceedings;…"*

***GCHQ functions***

9. By s. 3(1)(a) of the ISA [**Auths/tab 4**], the functions of GCHQ include the following:

> *"... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ...."*

10. By s. 3(2) of the ISA, these functions are only exercisable:

> *"(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*

*(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or*
*(c) in support of the prevention or detection of serious crime*."

11. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

> *"... that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."*

12. The functions of each of the Intelligence Services, and the purposes for which those functions may properly be exercised, are thus prescribed by statute. In addition, the duty-conferring provisions in section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of the ISA, otherwise known as *"the information gateway provisions"*, place specific statutory limits on the information that each of the Intelligence Services can obtain and disclose. These statutory limits apply to the obtaining and disclosing of information from or to other persons both in the United Kingdom and abroad.

**Counter-Terrorism Act 2008 [Auths/tab 9]**

13. By s.19(1) of the Counter-Terrorism Act 2008 ("CTA") *"A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions."*

14. By s. 19(2) of the CTA:

> "*Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*."

15. By s.19(3) to (5) of the CTA, information obtained by the Intelligence Services for the purposes of any of their functions may:

(a) In the case of the Security Service *"be disclosed by it – (a) for the purpose of the proper discharge of its functions, (b) for the purpose of the prevention or detection of serious crime, or (c) for the purpose of any criminal proceedings."* (s.19(3))

(b) In the case of SIS *"be disclosed by it – (a) for the purpose of the proper discharge of its functions, (b) in the interests of national security, (c) for the purpose of the prevention or detection of serious crime, or (d) for the purpose of any criminal proceedings."* (s.19(4))

(c) In the case of GCHQ "*be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings*." (s.19(5))

16. By s.19(6) any disclosure under s.19 "*does not breach* –

*(a) any obligation of confidence owed by the person making the disclosure, or*

*(b) any other restriction on the disclosure of information (however imposed)."*

17. Furthermore:

(a) s.19 does not affect the duties imposed by the information gateway provisions (s.19(7) and s.20(1) of the CTA).

(b) by s.20(2) of the CTA, nothing in s.19 "*authorises a disclosure that-*

*(a) contravenes the Data Protection Act 1998 (c.29), or*
*(b) is prohibited by Part 1 of the Regulations of Investigatory Powers Act 2000 (c.23)."*

18. Thus, specific statutory limits are imposed on the information that the Intelligence Services can obtain, and on the information that it can disclose under the CTA.

***Other statutory bases for obtaining information***

19. Information contained in a Bulk Personal Dataset may be obtained by other means, including pursuant to:

(a) Warrants issued under section 5 of the ISA in respect of property and equipment interference [**Auths/tab 4**];

(b) Authorisations issued under section 7 of the ISA in respect of property and equipment interference [**Auths/tab 4**];

(c) Intrusive surveillance warrants issued under section 43 of the Regulation of Investigatory Powers Act 2000 ("RIPA") [**Auths/tab 7**];

(d) Directed surveillance authorisations issued under section 28 of RIPA [**Auths/tab 7**];

(e) Covert human intelligence authorisations issued under section 29 of RIPA [**Auths/tab 7**]; and

(f) Warrants for the interception of communications issued under section 5 of RIPA [**Auths/tab 7**]

20. It is important to note that these other statutory means of obtaining information are themselves subject to their own statutory requirements, in addition to any further requirements derived from the Handling Arrangements set out below.

**The HRA [Auths/tab 6]**

21. Art. 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:

"*(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*

*(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevent of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others*."

22. By s. 6(1):

"*It is unlawful for a public authority to act in a way which is incompatible with a Convention right*."

23. Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, the Respondents must (among other things) act proportionately and in accordance with law. In terms of BPD-related activity, the HRA applies at every stage of the process i.e. authorisation/acquisition, use/access, disclosure, retention and deletion.

24. S. 7(1) of the HRA provides in relevant part:

"*A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may –*

*(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ....*"

**The DPA** [**Auths/tab 5**]

25. Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data that it holds. "Personal data" is defined in s.1(1) of the DPA as follows:

"*data which relate to a living individual who can be identified-*
*i. from those data; or*
*ii. from those data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.*"

26. Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.

27. Consequently as a data controller, the Respondents are in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from

the sixth data protection principle). Thus the certificates do not exempt the Intelligence Services from their obligation to comply with the fifth and seventh data protection principles, which provide:

> "*5. Personal data processed*[1] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …*
>
> *7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*."[2]

28. Accordingly, when the Respondents obtain any information which amounts to personal data, they are obliged:

    (a) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and

    (b) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

**The OSA** [**Auths/tab 2**]

29. A member of the Intelligence Services commits an offence if "*without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services*": s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of any of the Respondents that is *e.g.* in breach of the relevant "arrangements" (under s. 4(2)(a) of the ISA) will amount to a criminal offence. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).

30. Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

---

[1] The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

[2] The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

**Oversight mechanisms**

31. There are three principal oversight mechanisms in respect of the BPD Regime:

    (a) The Intelligence Services Commissioner; The Interception of Communications Commissioner;

    (b) The ISC; and

    (c) The Tribunal.

**The Intelligence Services Commissioner**

32. The Prime Minister is under a duty to appoint an Intelligence Services Commissioner (see s. 59(1) of RIPA [**Auths/tab 7**]). By s. 59(5), the person so appointed must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Commissioner is currently Sir Mark Waller.

33. The Intelligence Services Commissioner's remit under s.59(2) of RIPA is to provide independent oversight of the use of the powers contained within ss. 5 and 7 of ISA and Parts II and III of RIPA.

34. On 11 March 2015 the Prime Minister issued the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015 ("the Direction") [**Auths/tab 16**] pursuant to section 59A of RIPA. This was sent to the Intelligence Services Commissioner on 12 March 2015 and came into force on 13 March 2015.

35. Paragraph 5 of the Direction defines *"bulk personal dataset"* as meaning:

> *"any collection of information which:*
>
> *a. Comprises personal data as defined by section 1(1) of the Data Protection Act 1998;*
>
> *b. Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;*
>
> *c. Is held, or acquired for the purpose of holding, on one or more analytical systems within the Security and Intelligence Services."*

36. By paragraph 3 of the Direction, the Intelligence Services Commissioner is required to *"continue to keep under review the acquisition, use, retention and disclosure"* by the Intelligence Services of bulk personal datasets, *"as well as the adequacy of safeguards against misuse"*.

37. Paragraph 4 of the Direction provides that the Intelligence Services Commissioner must specifically *"seek to assure himself that the acquisition, use, retention and disclosure of bulk personal datasets does not occur except in accordance with section 2(2)(a) of the Security Service Act 1989, sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994"*. Paragraph 4 requires that, as part of this, the Intelligence Services Commissioner

must also "*seek to assure himself of the adequacy of the* [Respondents'] *handling arrangements and their compliance therewith.*"

38. Prior to the Direction being issued, the Intelligence Service Commissioner had overseen the acquisition, use, retention and disclosure of BPD on a non-statutory basis. This was acknowledged in paragraph 3 of the Direction ("*shall continue to keep under review…*").

39. Under s. 59(7) of RIPA, the Intelligence Services Commissioner must be provided with such staff as are sufficient to ensure that he can properly carry out his functions.

40. A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Intelligence Services Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 60(1) of RIPA.

41. In practice, the Intelligence Services Commissioner visits each of the Intelligence Services and the main Departments of State twice a year. Written reports and recommendations are produced after his inspections of the Intelligence Services. The Intelligence Services Commissioner also meets with the relevant Secretaries of State. In addition to the formal inspections, there is also regular engagement between the Intelligence Services Commissioner (and his office) and the Intelligence Services and relevant Departments of State on, for example, responding to Commissioner-led investigations or consulting on new guidance, draft legislation or any novel or contentious issue that would benefit from a view from the Commissioner.

42. S. 60 of RIPA imposes important reporting duties on the Intelligence Services Commissioner. (It is an indication of the importance attached to this aspect of the Intelligence Services Commissioner's functions that reports are made to the Prime Minister.)

43. The Intelligence Services Commissioner is by s. 60(2) of RIPA under a duty to make an annual report to the Prime Minister regarding the carrying out of his functions. He may also, at any time, make any such other report to the Prime Minister as he sees fit (s. 60(3)). Pursuant to s. 60(4), a copy of each annual report (redacted, where necessary under s.60(5)), must be laid before each House of Parliament. In this way, the Intelligence Services Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Intelligence Services Commissioner's practice is to make annual reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed openly.

44. In addition, the Intelligence Services Commissioner is required by s. 59(3) to give the Tribunal:

> "*…such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-*
>
> *(a) in connection with the investigation of any matter by the Tribunal; or*
>
> *(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter.*"

45. The Tribunal is also under a duty to ensure that the Intelligence Services Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).

46. It is to be noted that in the IPT judgment in the Liberty/Privacy proceedings, [2014] UKIPTrib 13_77-H dated 5 December 2014 [**Auths/tab 38**] the Tribunal placed considerable emphasis on the important oversight which is provided by the Interception Commissioner (see in particular §§24, 44, 91, 92 121 and 139 of the judgment) and a similarly important role is provided by the Intelligence Services Commissioner in the present context.

**The Interception of Communications Commissioner**

47. The Prime Minister must also appoint an Interception of Communications Commissioner (see s. 57(1) of RIPA). The statutory provisions in relation to the Interception of Communications Commissioner (hereafter referred to as "the Interception Commissioner") largely mirror those in respect of the Intelligence Services Commissioner, but are summarised below for the sake of convenience and because they differ in some respects from those relating to the Intelligence Services Commissioner.

48. By s. 57(5), the person appointed as Interception Commissioner must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Interception Commissioner is Sir Stanley Burnton.

49. The Interception Commissioner's remit under s.59(2) of RIPA is to provide independent oversight of the use of the powers contained within Part I of RIPA. He also has non-statutory oversight over the issue of directions pursuant to section 94 of the Telecommunications Act 1984.

50. Under s. 57(7) of RIPA, the Secretary of State must, after consultation with the Interception Commissioner, provide the Commissioner with such technical facilities available and staff as are sufficient to secure that the Commissioner can properly carry out his functions.

51. A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Interception Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 58(1) of RIPA.

52. In practice, the Interception Commissioner visits each of the Intelligence Services and the main Departments of State twice a year. Written reports and recommendations are produced after his inspections of the Intelligence Services. The Interception Commissioner also meets with the relevant Secretaries of State. In addition to the formal inspections there is also regular engagement between the Interception Commissioner (and his office) and the Intelligence Services and relevant Departments of State.

53. S. 58 of RIPA imposes important reporting duties on the Interception Commissioner. Again, as with the Intelligence Services Commissioner's reports, reports are made to the Prime Minister.

54. The Interception Commissioner is by s. 58(2) of RIPA under a duty to make an annual report to the Prime Minister regarding the carrying out of his functions. He must also make a report to the Prime Minister of any contravention of the provisions of RIPA in relation to any matter with which he is concerned, if it has not been the subject of a report made to the Prime Minister by the Tribunal (s. 58(2)) or if arrangements made under, inter alia, s.15 of RIPA (in relation to the use of intercept material and related communications data) have proved inadequate in respect of a matter with which he is concerned (s.58(3)). He may also, at any time, make any such other report to the Prime Minister as he sees fit (s. 58(5)(3)). Pursuant to s. 58(6), a copy of each annual and half-yearly report (redacted, where necessary under s.58(7)), must be laid before each House of Parliament. Again as in the case of the Intelligence Services Commissioner, in this way, the Interception Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Interception Commissioner's practice is to make his reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed openly.

55. The Interception Commissioner is required by s. 57(3) to give the Tribunal:

> "*…such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-*
> *(a) in connection with the investigation of any matter by the Tribunal; or*
> *(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter.*"

56. The Tribunal is also under a duty to ensure that the Interception Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).

57. The considerable emphasis placed by the Tribunal on the important oversight provided by the Interception Commissioner in the *Liberty/Privacy* IPT judgment [**Auths/tab 38**] (see in particular §§24, 44, 91, 92 121 and 139 of the judgment).

**The ISC**

58. The Security Service is responsible to the Home Secretary.[3] GCHQ and SIS are responsible to the Foreign Secretary.[4] The Foreign Secretary and Home Secretary are in turn responsible to Parliament. In addition, the ISC plays an important part in overseeing the activities of the Intelligence Services. In particular, the ISC is the principal method by which scrutiny by Parliamentarians is brought to bear on those activities.

59. The ISC was established by s. 10 of the ISA. As from 25 June 2013, the statutory framework for the ISC is set out in ss. 1-4 of and Sch. 1 to the Justice and Security Act 2013 ("the JSA") **[Auths/tab 10]**.

[3] The Director-General of the Security Service must make an annual report on the work of the Security Service to the Prime Minister and Home Secretary (s. 2(4) of the SSA).
[4] The Director of GCHQ must make annual reports on the work of GCHQ to the Prime Minister and Foreign Secretary (see s. 4(4) of the ISA).

60. The ISC consists of nine members, drawn from both the House of Commons and the House of Lords. Each member is appointed by the House of Parliament from which the member is to be drawn (they must also have been nominated for membership by the Prime Minister, following consultation with the leader of the opposition). No member can be a Minister of the Crown. The Chair of the ISC is chosen by its members. See s. 1 of the JSA.

61. The executive branch of Government has no power to remove a member of the ISC: a member of the ISC will only vacate office if he ceases to be a member of the relevant House of Parliament, becomes a Minister of the Crown or a resolution for his removal is passed by the relevant House of Parliament. See §1(2) of Sch. 1 to the JSA.

62. The current chair is Dominic Grieve QC MP. He is a former Attorney-General.

63. The ISC may examine the expenditure, administration, policy and operations of each of the Intelligence Services: s. 2(1). Subject to certain limited exceptions, the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions. See §§4-5 of Sch. 1 to the JSA. The ISC operates within the "ring of secrecy" which is protected by the OSA. It may therefore consider classified information, and in practice takes oral evidence from the Foreign and Home Secretaries, the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ, and their staff. The ISC meets at least weekly whilst Parliament is sitting. Following the extension to its statutory remit as a result of the JSA, the ISC is further developing its investigative capacity by appointing additional investigators.

64. The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers appropriate (s. 3(2) of the JSA). Such reports must be laid before Parliament (see s. 3(6)). They are as necessary redacted on security grounds (see ss. 3(3)-(5)), although the ISC may report redacted matters to the Prime Minister (s. 3(7)). The Government lays before Parliament any response to the reports that the ISC makes.

65. The ISC sets its own work programme: it may issue reports more frequently than annually and has in practice done so for the purposes of addressing specific issues relating to the work of the Intelligence Services.

66. It is to be noted that in the *Liberty/Privacy* judgment [**Auths/tab 38**], the Tribunal placed considerable emphasis on the important oversight which is provided by the ISC (see in particular §44 and §121 of the judgment); the Tribunal describing the ISC as "*robustly independent*" at §121.

**The Tribunal**

67. The Tribunal was established by s. 65(1) of RIPA [**Auths/tab 7**]. 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).

68. The Tribunal's jurisdiction is broad. As regards the BPD regime, the following aspects of the Tribunal's jurisdiction are of particular relevance:

(a) 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).

(b) The Tribunal may consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which 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 (ss. 65(2)(b), 65(4) and 65(5)(a) and (b) of RIPA).

69. Complaints of the latter sort must be investigated and then determined "by applying the same principles as would be applied by a court on an application for judicial review" (s. 67(3)).

70. Thus the Tribunal has jurisdiction to consider any claim against any of the Intelligence Services that it has obtained, used, accessed, retained or disclosed information in breach of the ECHR. Further, the Tribunal can entertain any other public law challenge to any such alleged acts or omissions in relation to information.

71. Any person, regardless of nationality, may bring a claim in the Tribunal. Further, a claimant does not need to be able to adduce cogent evidence that some step has in fact been taken by the Intelligence Services in relation to him before the Tribunal will investigate.[5] As a result, the Tribunal is perhaps one of the most far-reaching systems of judicial oversight over intelligence matters in the world.

72. Pursuant to s. 68(2), the Tribunal has a broad power to require a relevant Commissioner (as defined in s. 68(8)) to provide it with assistance. Thus, in the case of a claim of the type identified in §151 above, the Tribunal may require the Intelligence Services Commissioner (see ss. 59-60 of RIPA) and/or the Interception Commissioner (see ss. 57-58 of RIPA) to provide it with assistance.

73. S. 68(6) imposes a broad duty of disclosure to the Tribunal on, among others, every person holding office under the Crown.

74. 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 requiring the destruction of any records of information which are held by any public authority in relation to any person. See s. 67(7).

[5] The Tribunal may refuse to entertain a claim that is frivolous or vexatious (see s. 67(4)), but in practice it has not done so merely on the basis that the claimant is himself unable to adduce evidence to establish *e.g.* that the Intelligence Services have taken some step in relation to him. There is also a 1 year limitation period (subject to extension where that is "equitable"): see s. 67(5) of RIPA and s. 7(5) of the HRA.

**RIPA/ISA Codes of Practice**

75. As noted above at §19 BPDs may be obtained, inter alia, pursuant to warrants/authorisations issued under RIPA or ISA. The relevant statutory regimes themselves contain published safeguards (in relation to acquisition, retention, storage and destruction of material)) which are found in the following published Codes of Practice:

(a) Covert Human Intelligence Sources Codes of Practice (2002, 2010, 2014) [**Auths/tabs 65, 71 and 73**]:

(a) Tests of **necessity** and **proportionality** in relation to:

(i) Applications for and the granting of CHIS authorisations under Part II of RIPA: **2002 Code**: §§2.4-2.5, §4.14; **2010 Code**: §2.9, §§3.2-3.5, §§5.1-5.2, §5.10; **2014 Code**: §§3.4-3.5.

(ii) Renewal/cancellation of CHIS authorisations: **2002 Code**: §4.19, §4.25; **2010 Code**: §3.12, §3.14, §5.15, §5.18; **2014 Code**: §3.14, §3.16, §5.16, §5.18, §5.22, §5.28.

(b) Requirement to consider potential collateral intrusion: **2002 Code**: §§2.6-2.8, §4.19; **2010 Code**: §§3.8-3.11, §3.14, §5.10, §5.15; **2014 Code**: §§3.8-3.11, §3.16, §3.22.

(c) Safeguards in respect of disclosure, handling, copying and retention of intercepted material: **2002 Code**: §2.17; **2010 Code**: §8.1; **2014 Code:** §8.1; destruction: **2002 Code**: §2.17; **2010 Code**: §8.1; **2014 Code**: §8.1.

(b) Covert Surveillance and Property Interference Codes of Practice (2002, 2010 and 2014) [**Auths/tabs 66, 72 and 74**]:

(a) Tests of **necessity** and **proportionality** in relation to:

(i) Applications for covert / intrusive / directed surveillance warrants under Part II of RIPA/property interference warrants under s.5 ISA: **2002 Code**, §§2.4-2.5, §2.10, §§4.9-4.10, §§5.8-5.9, §5.16, §§6.6-6.7; **2010 Code**, §§3.3-3.6, §5.8, §§6.3-6.4, §6.19, §§7.10-7.11, §§7.37-7.38; **2014 Code**, §§3.3-3.6, §5.8, §§6.3-6.4, §6.19, §6.30, §§7.10-7.11, §7.38.

(ii) Renewal/cancellation of : **2002 Code**: §§4.23-4.26, §4.28, §§5.36-5.37; **2010 Code**, §5.12, §5.16, §6.30, §7.27, §7.30, §§7.40-7.42; **2014 Code**, §5.12, §5.16, §6.25, §6.32, §7.40.

(b) Requirement to consider potential collateral intrusion: **2002 Code**: §§2.6-2.8, §5.16, §6.27; **2010 Code**, §3.6, §§3.8-3.11, §6.19, §6.32; **2014 Code**, §§3.8-3.11, §7.18.

(c) Safeguards in respect of disclosure, handling, copying and retention

of intercepted material: **2002 Code**: §2.16; **2010 Code**: §9.3; **2014 Code**: §9.3); and destruction: **2002 Code**: §2.18; **2010 Code**: §9.3; **2014 Code**: §9.3.

(c) Equipment Interference Code of Practice (2016, but published in draft form in February 2015) [**Auths/tab 77**]:

(a) Tests of **necessity** and **proportionality** in relation to:

(i) Issuing of section 5 warrants/s.7 authorisations: §§2.4-2.8, §§4.6-4.7, §7.8, §7.13, ; and

(ii) Review/renewal/cancellation of s.5 warrants: §2.13, §§4.10-§4.13, §7.14, §7.17.

(b) Requirement to consider potential collateral intrusion: §§2.9-2.12.

(c) Safeguards in respect of disclosure, handling, copying and retention of material obtained by equipment interference: §3.13, §6.5, §6.7; storage (§6.8); destruction (§6.9).

(d) Interception of Communications Codes of Practice (2002 and 2016) [**Auths/tabs 64 and 76**]:

(a) Tests of **necessity** and **proportionality** in relation to

(i) Applications for and the granting of s.8(1)/s.8(4) warrants: **2002 Code**, §§2.4-2.5, §§4.2-4.3, §4.5, §§5.2-5.3, §5.5; **2016 Code**, §3.5-§3.7, §5.2-§5.5, §6.9-§6.11, §6.13.

(ii) Renewal/cancellation of s. .8(1)/s.8(4) warrants: **2002 Code**, §4.13, §5.12; **2016 Code**, §3.21; §5.14; §5.17; §6.22.

(b) Requirement to consider potential collateral intrusion: **2002 Code**, §3.1; §4.2; **2016 Code**, §4.1;

(c) Safeguards in respect of disclosure, handling, copying and retention of intercepted material (**2002 Code**, §6.2, §6.4; **2016 Code**, §7.3, §7.5-§7.6, §7.9); storage (**2002 Code**, §6.7, §7.7); destruction (**2002 Code**, §6.8, §7.8).

**Handling arrangements**

76. This section addresses the handling arrangements in place at GCHQ, MI5 and SIS from June 2005 onwards in relation to BPD. It does so by reference to the periods:

(a) Prior to the avowal of BPDs in the ISC's *Privacy and Security* report on 12 March 2015 (see **pages 15-35** below);

(b) From 12 March 2015 until the publication of the BPD Handling Arrangements on 4 November 2015 (see **pages 35-36** below);

(c) From 5 November 2015 to the date of the hearing; and

(d) As at the date of the hearing.

((c) and (d) are addressed together at **pages 36-44** below).

**a. Prior to the avowal of BPDs in the ISC's *Privacy and Security* report on 12 March 2015**

**i. GCHQ**

77. In this period, GCHQ's handling arrangements were set out in its Compliance Guide, relevant extracts from which are

(a) For the period June 2005 to 2010: at **[2/GCHQ1/89-146]**;
(b) For the period 2010 to June 2014: at **[2/GCHQ1/147-162].**
(c) For the period June 2014 to 4 November 2015: at **[2/GCHQ1/5-24**].

Acquisition

78. In relation to **acquisition** the Compliance Guide emphasised and explained the requirements that acquisition of be necessary and proportionate:

(a) For the period June 2005 to 2010, see **[2/GCHQ1/90-91, 110-111, 138]**; see e.g. at **90-91**:

*"4. In order to justify any interference with [Article 8] rights, a public authority must be able to demonstrate that the interference:*

- ***is prescribed by the law***

*...*

- ***has an aim which is legitimate under Article 8, paragraph 2***
  *– achieved if GCHQ's operations have, as their legitimate aim, one or more of the authorised purposes (which appears also in Article 8, paragraph 2);*
- ***is necessary in a democratic society***
  - *the necessary interference must be convincingly established and proportionate to the 'legitimate aim' being pursued;*
  - *the reasons given in justification must be both relevant and sufficient.*

***The Concept of Proportionality***

*5. While a public authority should not be unduly restricted in what it is trying to achieve legitimately, GCHQ's actions must constitute a proportionate means of securing achievement. In the first place, this means that, if other methods are available and these methods are equally effective but less intrusive, then the customer is bound to have considered these beforehand. Where action by GCHQ is the most appropriate method, it must be implemented with the minimum interference with Convention Rights in so far as the demands of the intelligence requirement and the knowledge available to GCHQ allow.*

*...*

*8. Because the potential effect of HRA is so wide, and because most SIGINT operations have an obvious potential to infringe someone's privacy, GCHQ's established policy is that every aspect of every GCHQ operation must conform to the principles expounded above."*

(b) For the period 2010 to June 2014 see:

(c) The "Analysis" section from June 2014 (at **[2/GCHQ1/148]**):

"***Bulk personal data***
*GCHQ acquires and stores some data sets that contain a high proportion of information relating to individuals. This data is either acquired lawfully from GCHQ's own collection operations, or from other parties. In the latter case, acquisition is authorised and recorded by obtaining a Data Acquisition Authorisation (DAA). Some of these data sets are classed as targeted bulk personal data sets i.e. they are personal because each record contains at least the name of an individual, but there is something about the data that implies a reasonable expectation that much of it will contain information of intelligence value to GCHQ. Some of these data sets are classed as non-targeted bulk personal data sets i.e. they are personal because each record contains at least the name of an individual, but the majority of the data is not believed to relate to probable intelligence targets. The relevant policy team makes the decision about what is targeted and non-targeted bulk personal data, in consultation with data owners."*

(d) The "Authorisations" section from November 2010 **[2/GCHQ1/150**]:

"***Acquisition of data from partners***
*GCHQ receives operational data from various sources other than its own collection operations...*
*Particular sensitivity attaches to any such data that includes details of non-targets as well as targets (i.e. is bulk in nature) and relates to identifiable individuals. You need to obtain a Data Acquisition Authorisation before you receive any operational data meeting these criteria from a partner. By following this process you will help to ensure that GCHQ's acquisition of the data is demonstrably necessary and proportionate..."*

(e) The "Authorisation" section for the period June 2014 to 4 November 2015 (at **[2/GCHQ1/7**]) repeated the text referred to at §78(d) above (updating the reference to "Data Acquisition Authorisation (DAA)" to "Bulk Personal Data Acquisition Request (BPDAR)") and added, in 2015:

*"When the Investigatory Powers Bill was published on 4 November 2015, new open arrangements covering the handling of Bulk Personal Data (BPD) and section 94*

*data across the SIA were published at the same time.*
*Complementing these open handling arrangements (which are unclassified) are sets of closed handling arrangements (classified SECRET) for BPD and Section 94 for each of the Security and Intelligence agencies (SIA) which took effect on 27 November 2015.*
*The introduction of these handling arrangements reflects the intention of the SIA to make the acquisition and use of BPD and section 94 data more transparent and subject to clearly articulated safeguards. It also responds to recommendations made by the Intelligence & Security Committee in its Privacy and Security Report and by David Anderson QC in his review of investigatory powers. The closed handling arrangements for GCHQ largely reflect current practices and policy although there are some minor changes.*
*All staff involved in work that involves the acquisition of BPD and/or section 94 material, or the handling of such material must follow these new handling arrangements."*

(f) In "Collection and data acquisition" **[2/GCHQ1/8]**:

*"GCHQ receives operational data from various sources other than its own interception. The principal sources are:*
*...*
*GCHQ treats all such data according to RIPA safeguards. This both demonstrates HRA compliance and enables systems to handle data consistently. You must ensure that there is appropriate authorisation in place to acquire data from these sources, in order to comply with the law or (in cases where no legal authorisation is needed) to demonstrate that its acquisition is necessary and proportionate. Further information is in 'Authorisations'.*
*..."*

(g) In the "Sharing" section at **[2/GCHQ1/19-20]**:

*"**Receiving Data***
*GCHQ receives operational data from many partner organisations.*
*...*
*You must handle any operational data obtained from partners in accordance with HRA and as if it were intercepted under RIPA. In particular, you must ensure that its acquisition is authorised, necessary and proportionate, and follow RIPA section 15 safeguards regarding access, review and retention. Particular sensitivity attaches to any such data that is bulk or unselected in nature (i.e. includes details of non-targets) and relates to identifiable individuals. You need to obtain a Data Acquisition Authorisation before you receive any operational data meeting these criteria from a partner. By following this process you will help to ensure that GCHQ's acquisition of the data is demonstrably necessary and proportionate."*

(h) Between June 2014 and January 2016 GCHQ used a designated form for acquisition of BPD, the "Authorisation for Acquisition of Bulk Personal Data" form **[2/GCHQ1/43-50]**. The form included, *inter alia*, questions about:

(a) The "Intelligence Case" for acquisition,

(b) Proposed retention period,

(c) Access controls,

(d) The "Extent of potential intrusiveness", including "Does the dataset contain a high proportion of data on people of no probable intelligence interest?", and an "Assessment of intrusiveness and sensitivity" **[2/GCHQ1/45**].

(e) The questions were to be answered by the "Data Owner" and assessed by a designated team. The authorising officer had to indicate that he/she was "satisfied that the acquisition of this dataset is necessary and proportionate in relation to one or more of GCHQ's authorised purposes and that it will be handled appropriately." **[2/GCHQ1/45**]

(i) Guidance was in force from October 2012 onwards **[2/GCHQ1/163] ;** see also the guidance from 1 June 2014 onwards at **[2/GCHQ1/51-58**]. This included guidance on how to describe the *"Intelligence case"* i.e. *"why [the Data Sponsor] believes it to be necessary and proportionate to hold bulk personal data of this nature and scale, and what he expects the likely intelligence benefits will be."* **[2/GCHQ1/164; see also [2/GCHQ1/57 and 53**]

Access/use

79. In relation to **access/use** GCHQ's Compliance Guide in the period June 2005 to 2010:

(a) Set out the general requirements relating to necessity and proportionality referred to above: §78(a).

(b) Sets out the responsibilities of reporters and analysts who wish to access data by applying a "selector" to it ("targeting") (at **[2/GCHQ1/95]**):

*"2. ...all targeting implemented on GCHQ systems still requires three categories of information that are mandatory:*

- ***the intelligence requirement*** [Redacted],
- ***the JIC Priority*** *and the* ***'authorised' purpose*** *of the requirement, i.e. in the interests of national security, to safeguard the economic wellbeing (EWB) of the UK, or for the prevention or detection of serious crime*
- ***the HRA justification for the targeting****, i.e. how the Targeting of this selector contributes reasonably to meeting the intelligence requirement(s) ('proportionality'). This does not equate to the intelligence requirement but explains why and how that requirement is being met by that targeting. That said, the link to the requirement might be self-evident from an official's position, or a ministry or agency name."*

*"5. Reporters and analysts have responsibility for checking that any tasking or selection terms which they have originated are in fact producing output proportionate to their intelligence requirement. Any tasking or selection which is not should be refined or deleted immediately. If such tasking or selection has constituted a breach of RIPA or the ISA, or of the safeguards associated with those Acts, the matter* ***must*** *be reported to line management for action."* (at **[2/GCHQ1/96]**)

80. In relation to **access/use** GCHQ's Compliance Guide in the period 2010 to June 2014 provided:

(a) The "Analysis" section stated:

> *"It is GCHQ policy to apply the same legal and policy handling rules to all operational data, whether it is acquired under [sic] by interception warrant or by any other means*
> *...*
> *To conduct analysis in a way that is fully compliant with the law, every search that you carry out must be:*
> - *authorised*
> - *necessary for one of GCHQ's purposes*
>
> *...*
> *and*
> - *proportionate.*
>
> *To demonstrate the necessity and proportionality of your search, you must supply an HRA justification. This consists of three parts:*
> - *JIC purpose eg 1 NS*
> - *Requirement number that equates to the intelligence requirement that your search seeks to meet*
> - *free-flow explicit textual justification that explains why you are carrying out this search.*
>
> *..."* **[2/GCHQ1/149]**

See also the material identical wording at **[2/GCHQ1/147-8]**

(b) Again, at **[2/GCHQ1/151]** *"GCHQ treats all such data according to RIPA safeguards. This both demonstrates HRA compliance and enables systems to handle data consistently."*

(c) The Compliance Guide in the period June 2014 to November 2015 (and until the present) included materially identical wording in its Analysis **[2/GCHQ1/6]**, Collection and data acquisition **[2/GCHQ1/8]**.

Disclosure

81. The Compliance Guide set out strict safeguards relating to disclosure as follows:

(a) In the period June 2005 to 2010, the "Special Responsibilities for Compliance" in relation to the "disclosure of information" were set out as follows at **[2/GCHQ1/97]**:

> *"8. The role and responsibilities of reporters and analysts are of central importance to the disclosure of information which has been acquired by GCHQ. Except in the cases of collaborating SIGINT liaison partners, information is normally issued to customers outside GCHQ only by way of formal intelligence report.*
>
> *9. In this way, GCHQ analysts and reporters release information:*

*– to UK recipients in order to satisfy HMG requirements;*
*– to non-UK recipients E.g. liaison partners to satisfy their requirements.*

*In each case, this release must be for [sic] necessary for one or more of the purposes authorised under ISA, i.e. in the interests of **national security** or the **economic well-being** of the UK (the actions or intentiosn of persons outside the British Islands), or in support of the prevention or detection of **serious crime**.*

*10. The report content must also observe the principle of proportionality in disclosing information only to the minimum extent necessary to satisfy the intelligence requirement, especially with regard to the amount of information disclosed and the level of detail that is provided. GCHQ analysts and reporters must also take care not to disclose certain categories of information at all, or to disclose it only after consultation and/or with special handling instructions."*

(b) Further, within the "Safeguards" section at **[2/GCHQ1/114]**:

*"* ***General Principles***
*1. Any information which is disclosed by GCHQ must meet a requirement that is based upon one of the authorised processes. The extent to which information is disclosed by GCHQ must be limited to the minimum **number of persons** that is relevant to the requirement which the provision of the information is intended to meet. It must also be limited to the minimum **extent** that is necessary to meet the authorised purpose.*
*2. These obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed, whether this is to additional persons within GCHQ or to persons outside GCHQ. Disclosure of information on any subject to organisations beyond GCHQ must be limited to those which have a requirement for it; disclosure by GCHQ must cease if and when the requirement for the information is withdrawn."*

(c) In the period 2010 to June 2014 the "Sharing" section of the Compliance Guide provided at **[2/GCHQ1/157-158]**:

*"**Principles***
*You may share operational data only if it is necessary for one of GCHQ's operational purposes. Your sharing must be kept to the minimum necessary and must be done in an approved, accountable way, in accordance with the guidance of this section. The legal basis for sharing is explained in overview.*
*If you wish to share a new line of data with an external organisation, you must first consult the relevant teams. Their judgment on the necessity of sharing will be taken within a broad context of policies associated with GCHQ's partnerships.*
*Staff and contractors seconded to or working for GCHQ are covered by the same legal requirements as GCHQ personnel, in particular ISA, HRA and RIPA. If you handle operational data you must be trained in operational legalities*
*...*
***Sharing GCHQ's data***
*You may share material derived from operational activity with other organisations, but this is subject to:*

- *legal safeguards*
- *policy approval*
- *accountability*

*The legal safeguards require that the sharing must be restricted to the minimum necessary for one of GCHQ's operational purposes and that receiving partners must accord the material protection equivalent to GCHQ's safeguards. If therefore you are contemplating sharing significant new lines of material with partners, and/or if you have any concerns relating to the equivalence of the safeguards that will be applied, you should refer the matter to the relevant policy team."*

The "Partnerships" section of the Compliance Guide was to similar effect (see **[2/GCHQ1/153-155**])

(d) In addition, the "Safeguards" section made clear (at **[2/GCHQ1/156**]) that:

*"reporting and other release of Sigint must be necessary and proportionate;"*

(e) In the period June 2014 to November 2015 the Compliance Guide was to materially identical effect as in the period 2010 to June 2014. See: "Partnerships" **[2/GCHQ1/16**]; "Safeguards" **[2/GCHQ1/18**] and "Sharing" [**[2/GCHQ1/20**].

(f) In addition from June 2014 onwards a "Data Sharing Request" form was in use **[2/GCHQ1/61-62; see also [2/GCHQ1/60-61**] for requests within the SIA to share BPDs. This included questions as to the "*Authorised statutory purpose*" and, "*Business case/justification (inc necessity and proportionality)"* to be filled out by the requesting agency. The agency to whom the request was made had to complete a "*response"* section, including explaining the "*Intrusion of the dataset"*. Guidance for the completion of the form was in force from June 2014 onwards **[2/GCHQ1/59-60**]

Retention/Review/Destruction

82. In addition, the Compliance Guide included the following safeguards in relation to retention/review/destruction:

(a) From June 2005 to 2010 the "Safeguards" section stated (at **[2/GCHQ1/123-124**]):

" ***Normal Periods for the Retention of Intercepted Material***

*3. For most categories of intercepted material, the following norms have been agreed. All material should be destroyed as soon as it can be determined reasonably that its retention is no longer necessary, and these time limits should be regarded as maxima unless retention beyond that time can be justified, after review, in acceptable terms (see below):"*

...

***The Retention of Information Beyond the Norms***

*4. Exceptional examples of retention beyond these norms may be occasioned routinely by areas of GCHQ which specialise in research and development."*

(b) At **[2/GCHQ1/125**]:

*"2. Any intercepted material which is retained beyond the norms must be reviewed*

*by analysts and reporters at appropriate intervals to confirm that is continued retention is justified. Justification should be in terms of one of the three authorised purposes allowed for by RIPA and by the ISA. Upon review, any records whose retention cannot be justified in these terms should be destroyed.*

*3. Where any material is retained for longer than the norms specified above, the reason for its continued retention must be recorded in local files, along with the next scheduled review date."*

(c) From 2010 to June 2014:

(a) The "Review and retention" section stated (at **[2/GCHQ1/155**]):

*"Principles*
*RIPA requires GCHQ to have arrangements to minimise retention of intercepted data and any material derived from it.*
*GCHQ implements this safeguard through policy by specifying maximum periods of retention for categories of Sigint and IA material; the policy also caters for exceptional needs.*
*Material kept beyond default periods must be reviewed and rejustified, in most cases annually.*
*GCHQ treats all operational data as if it were obtained under RIPA. Very little data is kept for legal purposes alone.*
*Retention limits*
*This Compliance Guide and the Operations Data Retention Policy (DRP) set out GCHQ's arrangements for minimising retention in accordance with the RIPA safeguards. The DRP achieves this by setting default maximum limits for storage of Operations data.*
*[REDACTED]"*

(b) The Safeguards section: *"RIPA requires GCHQ to have arrangements in place to minimise its retention and dissemination of intercepted material...GCHQ applies RIPA safeguards to all operational data."* **[2/GCHQ1/156**]

(d) From June 2014 to November 2015 the Compliance Guide was essentially unchanged: see Safeguards **[2/GCHQ1/18**]; and the "Review and retention" section which remained unchanged until October 2015 (**[2/GCHQ1/17]**), when it added: *"Retention of material beyond these default periods must be formally approved. Continued retention must be reviewed and rejustified, in most cases annually."* **[2/GCHQ1/17**]

(e) From June 2014 proposed retention of a BPD required to be justified in a specified form. This was "Section B" of the "Authorisation for Acquisition of Bulk Personal Data" form referred to at §78(h) above, and was headed "Review of Retention of Bulk Personal Data" **[2/GCHQ1/47-50**]

For the avoidance of doubt, the default retention periods referred to in the foregoing extracts from the Compliance Guide did not apply to BPD because the data in BPDs did not fall clearly into the relevant categories. BPDs were therefore considered on a case-by-case basis, applying RIPA safeguards.

83. In relation to destruction, as already noted, GCHQ treats all operational data (including BPD) according to RIPA safeguards. These include ensuring that material is destroyed as soon as its retention is no longer necessary for an authorised purpose: see Compliance Guide for June 2005 to 2010 **[2/GCHQ1/112; 123**]; Compliance Guide for 2010-June 2014, "Safeguards" **[2/GCHQ1/156**]; Compliance Guide for June 2014 onwards **[2/GCHQ1/18**].

February 2015 SIA BPD Policy

84. In February 2015 a joint "SIA Bulk Personal Data Policy" came into force **[1/MI51/309-317**]. This is addressed at §120 below.

### ii. Security Service

Acquisition

85. In October 2006 MI5 began to apply a "Bulk External Data Acquisition – Internal Authorisation Process" ("the 2006 policy") [**Core/B/2/MI5 statement, para. 57]; [1/MI51/177-180**]. This was initially used only by one part of MI5's data analyst team but by late 2006/early 2007 had been adopted throughout MI5. MI5's policy and practice followed this document, and used the "Bulk Data Acquisition Authorisation" form at [**1/MI51/185-188]** until October 2010.

86. The 2006 policy:

(a) Defined *"bulk data"* as *"Electronic data sets that are too large to be easily susceptible to manual processing and contain data about multiple individuals"* **[1/MI51/179**]

(b) Required all bulk data acquisition to be authorised by a MI5 officer of Grade 2 in the sponsoring section. However, if data was *"particularly intrusive"* the Grade 2 officer was to consider seeking the endorsement of a senior MI5 official (*ibid.*).

(c) The *"relevant form"* (as annexed at **[1/MI51/185-188**]) was to be used **[1/MI51/179**]. Any data ingested on to the BPD analytical system was to be accompanied by that form (*ibid.*).

(d) Created the role of "*section data coordinator"* [**Core/B/2/MI5 statement, §59; MI5 ex. 183**], with responsibility for, inter alia, reviewing the necessity/proportionality of retention of BPD.

(e) The relevant form included the following key questions:

(a) *"Proposed data retention period"*; *"Proposed retention review frequency (usually every 6 months)"* **[1/MI51/185**]

(b) *"Please describe how you intended to use the data and why this is necessary to help the Service to meet its statutory requirements to protect national security."* **[1/MI51/186]**

(c) *"Please explain the level of intrusion into privacy: (issues you should explore include – The nature of the data (it is personal data etc?) Does the database contain a high or low proportion of people of no intelligence interest? Is the data anonymous and will it remain so? [for example, could other data or techniques available to the Service be used to remove this anonymity?] Have you requested the totality of the database or a subset and does this help to manage intrusion? Who in the Service will have access to the data?"* **[1/MI51/186]**

(d) *"What results and benefits will exploiting this data bring and could these be achieved by other means without the use of bulk data?"* **[1/MI51/187]**

87. The form for acquisition continued to be revised and updated in the period 2006-2010: see version 1 of the Data Acquisition, Retention, Use and Release Questionnaire **[1/MI51/189-190]**; and the Form for Acquisition, v.3 **[1/MI51/191-195]**. The questions continued to be focused on ascertaining whether acquisition of BPD was necessary and proportionate.

88. In October 2010 MI5 issued the Policy for Bulk Data Acquisition, Sharing, Retention & Deletion ("the 2010 Policy") **[1/MI51/17-28]**. Acquisition was addressed at **[1/MI51/19-20].** Key statements in relation to acquisition were:

(a) *"All acquisition requests must be supported by a business case approved by a senior MI5 official from the intelligence section and must be supported by a data analysis and exploitation expert, known as 'data sponsors'."*

(b) *"A senior MI5 official will authorise the acquisition once he is satisfied that it is both necessary and proportionate for the Service to hold and use the dataset in pursuit of the Service's statutory function to protect national security. As part of this the senior MI5 official must be satisfied that any resulting interference with individuals' right to privacy, as enshrined in Article 8(1) European Convention on Human Rights (ECHR), is justifiable under Article 8(2) for the purpose of protecting national security."*

(c) *"All acquisition requests must be submitted on the relevant form."*

(d) *"Investigative sections and data sponsors must be able to justify the acquisition and subsequent retention and/or updates of a dataset as necessary and proportionate by weighing up, on the one hand, the business gains of having the information against, on the other hand, any resultant interference with privacy, also referred to as 'intrusion'."*

(e) *"Legal advisers' advice should be sought when evaluating whether the acquisition of a dataset is necessary and proportionate."*

(f) *"In some cases it may be necessary for the relevant team to approach the data provider to examine whether any unnecessary/extraneous parts of the dataset can be*

*removed prior to acquisition. Such extraneous data might include large numbers of minors, details of earnings or medical information."*

(g) *"The relevant team will also make a further assessment on the necessity and proportionality of acquiring the data, and will take into account the extent of political, corporate or reputational embarrassment and/or damage that compromise of the data would cause, including to the bulk data supplier."*

(h) *"Bulk Datasets may not be used without appropriate authorisation from senior MI5 officials...**Failure to follow the processes described in this policy may result in disciplinary action being taken**."*

89. Guidance on the meaning of "intrusion" and how to assess it was given at **[1/MI51/23-24]**.

90. The forms for acquisition were amended in November 2010 **[1/MI51/197-202]** and June 2014 **[1/MI51/203-210]** (see also [**Core/B/2/MI5 statement, §62**).

Access/use

91. The 2010 Policy **[1/MI51/17-28]** made clear under the heading "Permitted Use" that **[1/MI51/20]**:

(a) *"Access to Bulk Data is limited to those with a business need e.g. investigators, operational staff, data analysts and system administrators. Before access is granted all users must read and sign the relevant Code of Practice. They must also attend a compulsory training course that lasts two days (full time or integrated in other courses)."*

(b) *"All users must ensure that Bulk Data searches are necessary and proportionate to enable the Service to carry out its work and searches must be structured and targeted in a way that is most likely to select information relevant to the enquiry."*

Disclosure

92. The 2010 Policy **[1/MI51/17-28]** included provisions about sharing BPD at **[1/MI51/21]**:

*(a)* *"**Sharing Bulk Data with SIA Partners***
*Where GCHQ or SIS identify that a dataset owned by the Service would enable them to discharge their statutory functions, they should discuss their requirements with data sponsors...The data sponsor will complete the relevant form, which outlines the business case submitted by the requesting Agency, detailing the actual data requested, the necessity and proportionality of holding that data and data handling proposals. This must be approved by senior MI5 officials."*

*(b)* *"**Acquiring Bulk Data from SIA Partners***
*When an investigative section becomes aware of a bulk dataset held by SIS or GCHQ that might assist the Service in progressing our work, the investigative section must discuss their requirements and potential access to information with data sponsors. Formal applications for acquisition of bulk data from SIA partners must be submitted*

*on the appropriate form and authorised before being sent to the SIA partner. Once the relevant SIA partner is satisfied that the business case is justified and that sharing the data will not breach any security considerations that they may have arrangements will be made to share the data."*

See also **[1/MI51/27]**.

93. MI5 required a "Form for Sharing" to be completed. The form used from February 2011 is at **[1/MI51/809-812]**; The form used from January 2012 is at **[1/MI51/217-223]**; the form used from January 2014 to March 2015 is at **[1/MI51/225-231]** (see also [**Core/B/2/MI5 statement, §62]**).

Retention/Review/Destruction

94. MI5 had retention and review policies in place from 2006 onwards. As is apparent from the annex to the 2006 policy **[1/MI51/186-187**] the authorising officer stated the "proposed data retention period." Retention reviews were typically carried out every 6 months **[1/MI51/185**].

95. The 2010 Policy addressed review/retention/destruction as follows (at **[1/MI51/20-22 and 25]**):

(a) "***The Review Process***

*The Bulk Data Review Panel (BDR Panel) meets every 6 months to review all bulk datasets. The aim of the Panel is to ensure that Bulk Data has been properly acquired and its retention remains necessary and proportionate to enable the Service to carry out its statutory duty to protect national security for the purposes of s.2(2)(a) Security Service Act 1989. Panel members must satisfy themselves that the level of intrusion is justifiable under Article 8(2) of the ECHR and is in line with the requirements of the Data Protection Act 1998*

*The Bulk Data Review Panel is chaired by a senior MI5 official and operates under the authority of DDG (senior official responsible for the Service's operational capacity).*

*The Panel weighs up each dataset's usage over the 6 month period against necessity, proportionality, level of intrusion and the potential corporate, legal, reputational and political risk. The Panel also considers the frequency of acquisition and updates and whether such information could be acquired elsewhere by, for example, commercial means. The Panel decides whether to retain the dataset for a further 6 months or to delete it. In particularly sensitive cases, the Panel may recommend an earlier review. When the panel cannot agree on retention or deletion, the case will be referred to one of the Directors and ultimately the Director General for a decision."*

(b) "***Deletion of Data***

*Where the BDR Panel decides that a dataset should be deleted, the appropriate team will delete it within a reasonable timescale as specified by the Panel. The dataset will be deleted in its entirety. Deleted Bulk Data will not be archived."*

(c) Further detail was given at **[1/MI51/25-26]**.

96. More detailed supplementary guidance was given from October 2012 in MI5's "Bulk Data Retention and Deletion Policy" **[1/MI51/29-33**]. As summarised at [**Core/B/2/MI5 statement, §72]** this modified the approach to be taken by the BPD Review Panel at its 6-monthly meetings. In particular:

(a) Although it remained a requirement that a retention form had to be completed for each BPD for each 6 monthly meeting of the BPD Review Panel (and the retention forms for every BPD would be reviewed by the data governance team) at the BPD Review Panel meetings, the Panel would not consider every BPD held.

(b) Rather, as from October 2012 onwards, the Panel would review any new datasets acquired since the previous meeting, datasets giving rise to issues (eg lack of usage of held but not yet ingested) and any datasets not reviewed in the previous two years.

97. This change reflected the considerable number of datasets acquired by MI5 by 2012: [**Core/B/2/MI5 statement, §72(c)].**

98. Further, from October 2014 MI5 modified its review process further. The modifications can be seen in the Loose Minutes of 19 September 2014 **[1/MI51/813-818**] and 21 October 2014 **[1/MI51/819**] but were, in summary:

(a) To determine review periods for BPD by reference to: intrusion, corporate risk, usage and themes.

(b) In particular, intrusion and corporate risk were to be the primary determinants, such that:

(a) High intrusion or corporate risk would lead to a review every 6 months.

(b) Medium intrusion or corporate risk would lead to a review every 12 months.

(c) Low intrusion or corporate risk would lead to a review every 2 years.

(c) Additionally, in the event of low usage or any other concern, the BPD would be referred to the Panel for discussion.

99. Throughout the period the relevant forms were frequently revised and updated. See the "Form for Retention" as at the following dates:

(a) February 2010: **[1/MI51/787-790**].
(b) July 2010: **[1/MI51/791-794**].
(c) January 2012: **[1/MI51/795-798**].
(d) January 2013: **[1/MI51/799-802**].
(e) May 2014: **[1/MI51/239-243**].
(f) June 2014: **[1/MI51/245-248**].

The forms each focused on the requirements of necessity and proportionality, taking into account the degree of intrusion, including collateral intrusion.

February 2015 SIA BPD Policy

100. In February 2015 a joint "SIA Bulk Personal Data Policy" came into force **[1/MI51/309-317**]. This is addressed separately at §120 below.

### iii. SIS

Acquisition

101. In 2007 SIS developed a bulk personal dataset authorisation process following a review in summer 2007 [**Core/B/2/SIS statement, §§25**, **28**]. A *"Bulk Data Acquisition/Transformation Authorisation"* form **[2/SIS/91-92**] was created for use from 2007 onwards, and continued to be used until March 2012. The form:

(a) Defined bulk data as "electronic information on multiple individuals or organisations containing untargeted individuals and sought or processed for intelligence purposes." **[2/SIS/91**]

(b) Required that details as to the *"Proposed data retention period"* and *"Proposed review frequency (normally 6 monthly)"* be given **[2/SIS/91**].

(c) Required those completing the form to answer the following questions in relation to **necessity** and **proportionality**:

(a) *"Please describe how you intend to use the data and why this is necessary to help the Service to meet its statutory requirements to protect national security. Issues you should cover include: What is the intended use of this data? What results and benefits will exploiting this data bring and could these be achieved by other means without the use of bulk data? What JIC requirements will this meet?"* **[2/SIS/92**]

(b) *"Please explain the level of intrusion into privacy. Issues you should cover include – The nature of the data (it is personal data etc?) Does the database contain a high/low proportion of people of no intelligence interest? Is the data anonymous and will it remain so? [eg – lists of telephone numbers] Will you be acquiring the whole database or a relevant subset? Who in the Service will have access to the data?"* **[2/SIS/92**]

(d) The form also noted that *"Legal adviser endorsement should be sought by the authoriser if they feel that the request is particularly intrusive (eg the data includes large numbers of people of no intelligence interest or is extremely intrusive/delicate eg medical records)."*

102. In 2009 SIS put in place a written policy entitled "Bulk Data Acquisition and Exploitation" **[2/SIS/79-83**]. This provided a definition of *"bulk data" ("raw electronic*

*information on multiple individuals or organisations, which may contain the details of untargeted individuals and which is sought or processed for intelligence purposes."* (§1) It noted the potential interference with privacy:

> *"Acquiring and processing bulk data may entail greater interference with privacy. SIS must consier this intrusion carefully when assessing the necessity and proportionality of acquisition and exploitation."*

103. Further, it stated that:

(a) *"If there is a risk of embarrassment to HMG or if authorisation is required under the ISA, SIS will submit or seek other relevant authorisations on data acquisition. If a submission is unnecessary, the relevant SIS official is responsible for authorising bulk data acquisitions.. The relevant SIS official is also responsible for authorising the transformation into an exploitable form of data that has been acquired unsolicited...The Data Acquisition/Transformation Authorisation Form is in Appendix A"* (§8(a)).

(b) "*Data Acquisition*
*10...Teams are advised to co-ordinate acquisition with the relevant team, who can also advise on best practice. Data can also be obtained from GCHQ and BSS through the appropriate process*."

104. This policy was updated in November 2010: **[2/SIS/49-54]**.

105. The authorisation form was updated in March 2012: **[2/SIS/93-96]**. This was used for all BPD acquisition, contrary to the statement on the form that it was not required where an "existing oversight mechanism" applied: see **[Core/B/2/SIS statement, §29]**. The amendments to the form were in summary:

(a) New sections were incorporated for recording the presence of any personal data or data on UK nationals or minors.

(b) In addition to the section on necessity and proportionality, a new section was incorporated specifically requiring an assessment of actual and collateral intrusion.

(c) The acquisition officer was required to sign and date alongside the formal approval of a senior officer,

(d) The approval of a member of the legal team confirming that holding the data complied with ISA 1994, DPA 1998 and the Human Rights Act 1998 was mandatory.

106. The authorisation form was updated again as follows:

(a) In January 2013 **[2/SIS/97-100**]. The form removed the reference excluding BPD acquired under existing oversight mechanisms, reflecting the pre-existing practice. It also included a more detailed section on data intrusiveness to be completed by a member of SIS's data transformation team following an assessment of the data. This recorded the presence of any data

relating to protected characteristics or confidential information.

(b) In January 2014 the form's title was changed to "Authorisation of Bulk Personal Dataset" **[2/SIS/21-26]**. A definition of BPD was included. Tick boxes were also included for recording the presence of any categories of data deemed to be particularly intrusive. Where that was the case, the analyst was required to make a specific justification for retaining and exploiting the data.

107. In December 2014 SIS produced new "Bulk Personal Data: Guidance on the Authorisation Process:" **[2/SIS/13-19]**. This included guidance on the relevant law, the potential for intrusion into privacy, details of particularly intrusive categories of personal data, and guidance on actual and collateral intrusion.

Access

***Code of Practice***

108. A Code of Practice for use of SIS's BPD database came into force in August 2010 **[2/SIS/101-104]**. This was updated in April 2011 **[2/SIS/105-107]** and again in October 2014 **[2/SIS/37-40]**. All users of the database were required to sign and comply with the rules set out in the Code of Practice. It noted, inter alia, that:

(a) *"To do their jobs, the database users are given access to a wide range of data, which will include many individuals of no intelligence interest. For this reason searching and using bulk data are particularly sensitive activities, requiring careful consideration and strict adherence by users to that which is necessary and proportionate to their work."* **[2/SIS/101]**

(b) *"The database must not be a 'free for all'. Users will have potential access to sensitive material. The Service's information policy and practices are designed to be compliant with the law, which dictates that users' actual access to information is limited to that which is necessary and proportionate for their work. Misuse of information, including unjustified and/or inappropriate access, would be unlawful and could in some circumstances constitute a criminal offence."* **[2/SIS/102]**

***Applications for access***

109. SIS staff wishing to apply for an account on the SIS database were required to submit a written justification on their request for access. The form in use before October 2011 is at **[2/SIS/109]**. In October 2011 the form was amended **[2/SIS/45-46]** and added the following question:

> *"The database contains sensitive personal data and access to it is controlled. Please explain why your post requires access and how it will provide operational value. Please provide 2 or 3 lines, briefly describing how you might use the database."*

110. In October 2014, the application form was updated to read as follows **[2/SIS/47]**:

> *"The database contains sensitive personal data, including on individuals who are not deemed to be of intelligence interest. Given the potential for intrusion into privacy, access to the application is controlled and only extended to users whose access to the*

*data is necessary and proportionate to the Service's functions in law. Access to the database is specific to an individual's role and will be removed when you change post, after which you would be required to re-apply for access, if necessary, based on your new role.*

*...*

*Please explain why your use of the database would be necessary for the Service toe exercise its functions for the purposes of national security, the economic wellbeing of the UK or the detection/prevention of serious crime:*

*...*

*How would your use of the database be proportionate to fulfilling the Service's functions – for example is there a less intrusive way for you to achieve the same objective without access to the database data?"*

***In-built safeguards***

111. Further, there were in-built safeguards in the electronic interface. At the following times the login prompt for the database read as follows [**Core/B/2/SIS statement, §§42-46**]:

(a) Between 2009 and June 2011:

*"This system may be used for authorised purposes only. All information on it belongs to HMG and may not be accessed without prior authorisation. The Service will audit and monitor information on this system. An individual user has no legal right to absolute privacy on this system. Any misuse of this system will be handled as a disciplinary matter. By continuing to logon you consent to these conditions."*

(b) Between June 2011 and October 2014:

*"Access to the database is strictly controlled and all searches subject to scrutiny by the Intelligence Services Commissioner and Security Department. You should ensure that your use of the system is related to your work and that using the database is necessary and proportionate. Misuse of the database data could amount to criminal offence and may lead to disciplinary action..."*

(c) Since October 2014:

*"Your access to and use of the data in the database are likely to represent an intrusion into individuals' privacy. The Human Rights Act requires your actions to be necessary for the purposes of SIS's functions and proportionate to what we are seeking to achieve. All queries require a justification that explains clearly why this search contributes to meeting a specified intelligence requirement.*

*Access to the database is strictly controlled and all searches subject to scrutiny by the Intelligence Services Commissioner and Security Department. You should ensure that your use of the system is related to your work and that using the database is necessary and proportionate. Misuse of the database data, including unjustified and/or inappropriate access, would be unlawful and could amount to a criminal offence. The Service will take disciplinary action where the database data is searched inappropriately by staff.*

*All users have signed the database Code of Practice and by clicking 'Accept' you are reconfirming your agreement to abide by it."*

112. Further, since October 2014, prior to running a search, users must provide a justification for running it [**Core/B/2/SIS statement, §47**].

***Internal guidance on Intranet/User Communications***

113. In addition, guidance on access to/use of BPD has been provided to users by means of SIS's "User Communications" **[2/SIS/85-89; 55-56**] and "Intranet pages" **[2/SIS/57-63]**. Relevant guidance in relation to access/use in the period 2009-March 2015 included:

(a) *"4. A name or other identifying detail contained within a data set is only revealed by a search for that detail, or for someone or something associated with it. And, as with other SIS records, we may only search for and access information for legitimate reasons."* (SIS Notice to all staff 2 October 2009 **[2/SIS/85**])

(b) "*SIS POLICY ON ACQUIRING, EXPLOITING AND RETAINING BULK PERSONAL DATA*

*...*

*We remind all database users that it, like other SIS data systems, may only be searched for official business reasons. Misuse of information in the database, including unjustified and/or inappropriate access, would be unlawful and could in some circumstances constitute a criminal offence.*

*The policy explains the potential intrusiveness of the datasets held and the various ways in which the Service mitigates this (whilst permitting database users to search across all datasets)."* (SIS Notice to all staff 5 November 2010 **[2/SIS/86]**)

(c) *"Please remember that every search has the potential to invade the privacy of individuals, including the privacy of individuals who are not the main subject of your search, so please make sure you always have a business need to conduct that search and that the search is proportionate to the level of intrusion involved."* (Database newsletter of 8 September 2011, including list of "Do's and don'ts" **[2/SIS/87**])

(d) "*MISUSE OF SIS BULK DATA*

*...*

*All users given access to SIS systems should search data only when they are satisfied it is necessary and proportionate to do so, and in support of the Service's statutory functions;*

*Deliberate or serious abuse of SIS systems could amount to gross misconduct and may result in dismissal."* (Notice to all staff 24 November 2011 **[2/SIS/88**])

Disclosure

114. SIS's "Bulk Data Acquisition and Exploitation" policy of 2009 **[2/SIS/79-83**] provided as follows in relation to disclosure/sharing of BPD:

(a) "*14. Information derived from data exploitation may be shared with other UK intelligence agencies, subject to appropriate source protection and handling caveats. Before passing data to a third party, staff must consult the Data Owner for Action On approval and an appropriate form of words...*"

*(b)* "***DATA SHARING***

*16. Bulk data is shared between SIS, GCHQ and BSS through the relevant process, managed by the appropriate team. This records what has been shared, covers the legal and policy basis for sharing and ensures that there are appropriate security controls. Sharing with UK agencies outside the relevant process requires Data Owners to be satisfied that these conditions have been met. In summary: an audit trail needs to be kept of data shared; sharing should serve a justifiable purpose and be proportionate to it; and the data must be securely held. The appropriate team, legal advisers and security officers can advise. Data must not be shared without the Data Owner's authorisation.*

*17. Bulk data can be shared with other parties (eg a liaison partner) with the Data Owner's permission and subject to certain assurances. Were there to be such sharing, the assurances would require a liaison to handle the data securely, not to share it further without permission, and to share, as far as is practicable ,results that have an impact on UK National Security.*

*18. Were data to be acquired from joint operations with partners (e.g. GCHQ/SIS operations), that data may be shared by the partner organisation without additional written legal assurances from SIS. Those parties involved are deemed to have jointly acquired the data and are both regarded as the data owner. Good practice requires* that reliable records are kept on what data has been sent where."

115. The updated November 2010 policy was materially identical in this regard: **[2/SIS/52]**.

116. An *"Inter-agency Bulk Data Sharing Form"* was in use from January 2007, which required details of, inter alia, the intrusion of the dataset to be set out. **[2/SIS/120**]. It was amended in August 2010 **[2/SIS/119**]. This required details of the *"authorised statutory purpose"* and *"Business case/justification (inc necessity and proportionality)"* and had to be authorised by a senior SIS official.

Retention/review/destruction

117. SIS's 2009 *"Bulk Data Acquisition and Exploitation"* policy **[2/SIS/79-83**] stated as follows (**at [2/SIS/82]**):

"***DATA RETENTION REVIEW***

*20. To comply with legal obligations, a senior SIS officer is responsible for ensuring that bulk datasets on the database are reviewed every six months. The review body should include a senior SIS officer, a Legal Adviser...and a member of the relevant*

*team. External attendees may be invited on an ad hoc basis at SIS discretion. Data is reviewed, against set criteria and assessments of both its intrusiveness and sensitivity, to ensure that:*

*(a) Data was acquired in lawful exercise of an SIS function;*

*(b) Each dataset is up to date for the purposes of exploitation, and does not comprise redundant or inaccurate data;*

*(c) Based on necessity and proportionality, and taking into account its utility, data needs to be retained (on the database or in storage) or destroyed.*

*21. The review mechanism will articulate the reason for each decision and its compliance with UK law. Data Owners will be consulted before any changes are made.*

*22. Some datasets may be unique (e.g. if repeat access is not guaranteed) but become obsolete or of little worth. However, if it is likely that they may be of future use, data can be retained off the database in storage. If a dataset has been completely replaced by a newer version, the older version will be destroyed."*

118. The updated November 2010 policy was materially identical in this regard: **[2/SIS/52-3]**.

February 2015 SIA BPD Policy

119. In February 2015 a joint "SIA Bulk Personal Data Policy" came into force **[1/MI51/309-317**]. This is addressed separately at §120 below.

SIA Bulk Personal Data Policy

120. The SIA Bulk Personal Data Policy came into force in February 2015 **[1/MI51/309-317**]. This provided a definition of bulk personal data (§2), and set out arrangements for **acquisition** (§§12-13), **use** (§§14-15), **sharing** (§§16-17), **retention** (§§18-19) and **deletion/destruction** (§§20-21). These included (but were not restricted to):

(a) **Acquisition**: this was to be authorised by a senior manager within the relevant agency; a request to obtain a dataset had to be justifiable and deemed necessary and proportionate in pursuit of the agency's statutory functions; acquisition of BPD had to be authorised before any analytical exploitation; all BPD was to be assessed to determine the levels of intrusion and corporate risk; robust access controls were to be imposed (§12).

(b) **Use**: agencies were to consider the different levels and types of intrusion and sensitivities inherent in the exploitation of BPD access to analytical systems was to be restricted to those with a business need; relevant training was to be completed; all use of BPD in whatever context was to be necessary and proportionate to enable the agency to fulfil its statutory obligations; users had to ensure their queries against BPD were structured and focused so as to minimise collateral intrusion; appropriate disciplinary action was to be taken against any person identified as abusing or misusing analytical capabilities or

BPD (§14).

(c) **Sharing**: when sharing, the supplying agency was to be satisfied that it was necessary and proportionate to share the data, and the receiving agency that it was necessary and proportionate to receive it; no BPD were to be shared with non-SIA third parties without prior agreement of the acquiring agency; were BPD to be shared with overseas liaison the relevant necessity and proportionality tests for onwards disclosure under the SSA/ISA would have to be met (§16).

(d) **Retention**: the necessity and proportionality of continued retention of BPD was to be reviewed by each agency; each agency had a review panel which would review BPD retention by that agency. The panel sat once every six months; the frequency of retention reviews varied across the agencies but all periods were determined by similar factors, including potential use, levels of intrusion; and levels of sensitivity or corporate risk (§18).

(e) **Deletion/Destruction**: the review panel would instruct the deletion/destruction of BPD when its retention was no longer necessary or proportionate; the panel can request the deletion/destruction of certain fields/criteria from within a dataset if they are not deemed to be necessary and proportionate whilst retaining the remainder of the dataset; the agencies' relevant technical sections are responsible for conducting the deletion/destruction of the BPD (§20).

**b. From 12 March 2015 until the publication of the BPD Handling Arrangements on 4 November 2015**;

**i. GCHQ**

121. The SIA BPD Policy referred to at §120 above was in force in this period.

122. The relevant provisions of GCHQ's Compliance Guide, and forms and related guidance in this period set out at §§§78-83 above were also still in force.

123. In addition, Terms of Reference for the BPD Review Panel came into force in March 2015: **[2/GCHQ1/63-64]**.

**ii. MI5**

124. As stated above, the SIA BPD Policy referred to at §120 above was in force in this period. In March 2015 internal MI5 Bulk Personal Data Guidance **[1/MI51/35-46]** came into force which reflected the SIA BPD Policy, but gave staff more detailed internal guidance.

125. New versions of the relevant BPD forms began to be used in this period:

(a) A new version of the Form for Acquisition began to be used in August 2015: **[1/MI51/211-216]**.

(b) A new version of the Form for Sharing began to be used in March 2015:

**[1/MI51/233-238]**.

(c) New versions of the Form for Retention began to be used in March 2015 **[1/MI51/249-252]**, May 2015 **[1/MI51/253-257]** and July 2015 **[1/MI51/259-263]**.

**iii. SIS**

126. As already stated, the SIA BPD Policy referred to at §120 above was in force in this period.

127. In addition:

(a) The "Bulk Personal Data: Guidance on the Authorisation Process" was updated in October 2015: **[2/SIS/5-11]**.

(b) A new version of the Authorisation of Bulk Personal Dataset form began to be used in October 2015: **[2/SIS/27-32]**.

(c) An updated review and retention policy was used from October 2015: **[2/SIS/131-134]**. This assigned BPDs to a review period based on their level of intrusion.

(d) Users of the database were required to confirm when carrying out a search that [**Core/B/2/SIS statement, §48**]:

*"I consider this search to be proportionate and there is no less intrusive means to achieve the same objective."*

**c. from 4 November 2015 to the date of the hearing**
**and**
**d. as at the date of the hearing**

BPD Handling Arrangements

128. On 4 November 2015 the BPD Handling Arrangements were published **[2/GCHQ1/183-193]**. These applied to each of GCHQ, MI5 and SIS.

129. The BPD Handling Arrangements apply to obtaining, use and disclosure of "bulk personal datasets" (§1.2) as defined at §2.2:

*"2.2 Among the range of information collected is **data that contain personal information about a wide range of individuals, the majority of whom are unlikely to be of any intelligence interest**. Typically these datasets are very large, and of a size which means they cannot be processed manually. Such datasets are referred to as **bulk personal datasets**. For the purposes of these Handling Arrangements, a 'bulk personal dataset' means any collection of information which:*

*(a) Comprises personal data;*

*(b) Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest; and*

*(c) Is held, or acquired for the purpose of holding, on one or more analytical systems within the Intelligence Services."*

130. "Personal data" is defined as having the meaning given to it in s.1(1) of the Data Protection Act 1998 (§2.3), but additionally includes data related to the deceased.

131. The purpose of the acquisition and use of BPD is explained at §§2.4-2.5:

*"2.4 Bulk personal datasets may be acquired through overt and covert channels. Such datasets provide information about subjects of intelligence interest ("subjects of interest"), but inevitably also include information about those who are of no direct relevance to Intelligence Service operations. It is not possible to acquire the information that will be of direct value to these operations without also acquiring this additional data; indeed, at the point of acquisition it may not be known exactly which information will prove to be of value.*

*2.5 The Intelligence Services draw on this data and use it in conjunction with other data in order to perform their functions, for example, to identify subjects of interest, validate intelligence or to ensure the security of operations or staff. It may also be used to facilitate the exclusion of individuals from an investigation or in pursuit of other intelligence requirements. This ensures that the activities of the Intelligence Services are correctly and solely focused on those individuals or organisations that are relevant to the performance of their statutory functions."*

132. The requirement that acquisition, use, retention and disclosure of BPD have *"clear justification, accompanied by detailed and comprehensive safeguards against misuse"* and be *"subject to rigorous oversight"* is made clear (§2.6). The BPD Handling Arrangements are intended to provide such safeguards (§2.7) and must be complied with, along with the requirements of the information gateway provisions:

*"Staff must ensure that no bulk personal dataset is obtained, used, retained or disclosed* ***except in accordance with the information gateway provisions*** *and* ***these Arrangements.****"*

133. The BPD Handling Arrangements apply to BPD *"howsoever obtained"*, that is through whichever of the variety of statutory powers by which the Intelligence Services are entitled to obtain it (§§2.8-2.9) without prejudice to *"additional applicable statutory requirements"* which apply in the case of some statutory powers (§2.9).

134. The BPD Handling Arrangements set out provisions in respect of each of the stages of the lifecycle of a Bulk Personal Dataset.

Authorisation and Acquisition

135. The key requirements on staff of the Intelligence Services before obtaining BPD are set out at §4.2:

*"based on the information available to them at the time, staff should always:*

- *be satisfied that the objective in question falls within the Service's statutory functions;*
- *be satisfied that it is **necessary** to obtain and retain the information concerned in order to achieve the objective;*
- *be satisfied that obtaining and retaining the information in question is **proportionate** to the objective;*
- *be satisfied that only as much information will be obtained as is **necessary** to achieve that objective."*

136. Clear guidance is provided to staff on the considerations of **necessity** and **proportionality**:

***"When will acquisition be "necessary"?***

*4.3 What is **necessary** in a particular case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the '**necessity**' requirement in relation to acquisition and retention, staff must consider why obtaining the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of the relevant Intelligence Service. In practice this means identifying the intelligence aim which is likely to be met and giving careful consideration as to how the data could be used to support achievement of that aim.*

***The obtaining must also be "proportionate"***

*4.4 The obtaining and retention of the bulk personal dataset must also be **proportionate** to the purpose in question. In order to meet the '**proportionality**' requirement, staff must balance (a) the level of interference with the individual's right to privacy, both in relation to subjects of interest who are included in the relevant data and in relation to other individuals who are included in the data and who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the data. Staff must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the data and the importance of the objective to be achieved. Staff must also consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion.*

*4.5 These can be difficult and finely balanced questions of judgement. In difficult cases staff should consult line or senior management and/or legal advisers for guidance, and may seek guidance or a decision from the relevant Secretary of State."*

137. A formal procedure must be followed prior to any acquisition or use as set out at §§4.6 to 4.7:

*"4.6 Before a new dataset is loaded into an analytical system for use, staff in each Intelligence Service must consider the factors set out in paragraph 4.2 based on the information available to it at the time. Each Agency has a rigorous formal internal authorisation procedure which must be complied with, except in those cases where the acquisition is already authorised by a warrant or other legal authorisation issued by a Secretary of State.*

*4.7 Staff in each Intelligence Service must always complete the formal internal authorisation procedure before the dataset is loaded into an analytical system for use. The authorisation*

*procedure involves an application to a senior manager designated for the purpose which is required to set out the following:*

- *a description of the requested dataset, including details of the personal data requested, and any sensitive personal data;*
- *the operational and legal justification for acquisition and retention, including the purpose for which the dataset is required and the necessity and proportionality of the acquisition;*
- *an assessment of the level of intrusion into privacy;*
- *the extent of political, corporate, or reputational risk;"*

138. Thus, the need to consider the key matters set out at §4.2 of the BPD Handling Arrangements, and explained at §§4.3-4.3, is built into the formal authorisation procedure.

139. There is a requirement to consult the legal advisers of the relevant Intelligence Service "*on all new BPD acquisitions*" and to have "*confirmed the legality of the acquisition and its continued retention before authorisation to use the dataset is given.*" (§4.8)

140. A record of the application for authorisation must be kept:

*"4.9 Once authorised, the completed application must be stored on a central record by the appropriate Intelligence Service's information governance/compliance team, which will include the date of approval. This record must also contain the date of acquisition of the relevant data, which should be the date used for the review process (for which see paragraph 7.1-7.5 below)."*

141. Thus the reasons why the acquisition was authorised, including the key considerations set out at §4.2, are available to be reviewed or audited in the future.

Access/Use

142. The BPD Handling Arrangements emphasise the high priority that is put on data security and protective security standards, on confidentiality of data, and on preventing/disciplining misuse of such data:

*"5.1 Each Intelligence Service attaches the highest priority to maintaining data security and protective security standards. Moreover, each Intelligence Service must establish handling procedures so as to ensure that the integrity and confidentiality of the information in the bulk personal dataset held is fully protected, and that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that appropriate disciplinary action is taken. In particular, each Intelligence Service must apply the following protective security measures:*

- *Physical security to protect any premises where the information may be accessed;*
- *IT security to minimise the risk of unauthorised access to IT systems;*

- *A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy."*

143. Specific, detailed measures are also set out which are designed to limit access to data to what is necessary and proportionate, to ensure that such access is properly audited, and to ensure that disciplinary measures are in place for misuse:

*"5.2 In relation to information in bulk personal datasets held, each Intelligence Service is obliged to put in place the following additional measures:*

- *Access to the information contained within the bulk personal datasets must be strictly limited to those with an appropriate business requirement to use these data;*
- *Individuals must only access information within a bulk personal dataset if it is necessary for the performance of one of the statutory functions of the relevant Intelligence Service;*
- *If individuals access information within a bulk personal dataset with a view to subsequent disclosure of that information, they must only access the relevant information if such disclosure is necessary for the performance of the statutory functions of the relevant Intelligence Service, or for the additional limited purposes described in paragraph 3.1.4 above;*
- *Before accessing or disclosing information, individuals must also consider whether doing so would be proportionate (as described in paragraphs 4.4 above and 6.3 below). For instance, they must consider whether other, less intrusive methods can be used to achieve the desired outcome;*
- *Users must be trained on their professional and legal responsibilities, and refresher training and/or updated guidance must be provided when systems or policies are updated;*
- *A range of audit functions must be put in place: users should be made aware that their access to bulk personal datasets will be monitored and that they must always be able to justify their activity on the systems;*
- *Appropriate disciplinary action will be taken in the event of inappropriate behaviour being identified; and*
- *Users must be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution."*

144. In addition, Intelligences Services are required to take specific measures "*to reduce the level of interference with privacy arising from the acquisition and use of bulk personal datasets*" (§5.3). Specifically:

*"5.3 The Intelligence Services also take the following measures to reduce the level of interference with privacy arising from the acquisition and use of bulk personal datasets:*

- *Data containing sensitive personal data (as defined in section 2 of the DPA) may be subject to further restrictions, including sensitive data fields not being acquired, sensitive fields being acquired but suppressed or deleted, or additional justification required to access sensitive data fields. In addition, the Intelligence Services may expand the list of sensitive data fields beyond those provided for in section 2 of the DPA to provide additional protection where appropriate.*

- *Working practice seeks to minimise the number of results which are presented to analysts by framing queries in a proportionate way, although this varies in practice depending on the nature of the analytical query;*

- *If necessary, the Intelligence Services can - and will - limit access to specific data to a very limited number of analysts."*

Disclosure

145. The disclosure of BPD outside the Intelligence Service which holds it can only occur if certain conditions are complied with:

*"6.1 Information in bulk personal datasets held by an Intelligence Service may only be disclosed to persons outside the relevant Service if the following conditions are met:*

- *that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;*
- *that it is **necessary** to disclose the information in question in order to achieve that objective;*
- *that the disclosure is **proportionate** to the objective;*
- *that only as much of the information will be disclosed as is **necessary** to achieve that objective."*

146. Again, guidance is given to staff on the requirements of **necessity** and **proportionality**. This is in terms which are similar to those set out at §§4.3-4.4 in relation to acquisition, but with particular reference to disclosure:

*"**When will disclosure be necessary?***

*6.2 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.*

***The disclosure must also be "proportionate"***

*6.3 The disclosure of the bulk personal dataset must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff must be satisfied that the level of interference with the individual's right to privacy is justified by the benefit to the discharge of the Intelligence Service's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole bulk personal dataset."*

147. Prior to any disclosure of BPD, staff must also take reasonable steps to ensure the intended recipient organisation *"has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data and ensuring that it is securely handled"* or have received satisfactory assurances from the intended recipient with respect to such arrangements (§6.4). This applies to all disclosure, including to other Agencies (§6.5),

and whether disclosure is of an entire BPD, a subset of a BPD or an individual piece of data from a BPD (§6.6).

148. Disclosure of the whole or subset of a BPD is subject to internal authorisation procedures in addition to those that apply to an item of data (§6.7):

*"The authorisation process requires an application to a senior manager designated for the purpose, describing the dataset it is proposed to disclose (in whole or in part) and setting out the operational and legal justification for the proposed disclosure along with the other information specified in paragraph 4.7, and whether any caveats or restrictions should be applied to the proposed disclosure. This is so that the senior manager can then consider the factors in paragraph 6.1, with operational, legal and policy advice taken as appropriate. In difficult cases, the relevant Intelligence Service may seek guidance or a decision from the Secretary of State."*

Review of Retention and Deletion

149. The Intelligence Services are each required to keep the justification for continued retention and use of BPD under review, as set out at §§7.1-7.2:

*"7.1 Each Intelligence Service must regularly review the operational and legal justification for its **continued retention and use** of each bulk personal dataset. Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies of it held within the relevant Intelligence Service must be deleted or destroyed.*

*7.2 The retention and review process requires consideration of the following factors:*

- *The operational and legal justification for continued retention, including its necessity and proportionality;*
- *Whether such information could be obtained elsewhere through less intrusive means;*
- *An assessment of the value and examples of use;*
- *Frequency of acquisition;*
- *The level of intrusion into privacy;*
- *The extent of political, corporate, or reputational risk;*
- *Whether any caveats or restrictions should be applied to continued retention."*

150. Thus, the justification for the retention of BPD, including whether it remains necessary and proportionate, the level of intrusion into privacy, and whether such information could be obtained elsewhere less intrusively, is not simply considered at the stages of acquisition, use or disclosure, but is kept under continuing review.

Other management controls

151. §§8.1-8.2 set out the requirement for each Agency to have an internal Review panel which scrutinises the acquisition, disclosure and retention of BPD:

*"8.1 The acquisition, retention and disclosure of a bulk personal dataset is subject to scrutiny in each Intelligence Service by an internal Review Panel, whose function is to ensure that each bulk personal dataset has been properly acquired, that any disclosure is properly justified, that its retention remains necessary for the proper discharge of the relevant Service's statutory functions, and is proportionate to achieving that objective.*

*8.2 The Review Panel in each Intelligence Service meets at six-monthly intervals and are comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams."*

152. In addition, use of BPD is monitored by an audit team within each Agency:

*"8.3 Use of bulk personal data by staff is monitored by the relevant audit team in each Intelligence Service in order to detect misuse or identify activity that may give rise to security concerns. Any such identified activity initiates a formal investigation process in which legal, policy and HR (Human Resources) input will be requested where appropriate. Failure to provide a valid justification for a search may result in disciplinary action, which in the most serious cases could lead to dismissal and/or the possibility of prosecution."*

153. §8.4 notes that all reports on audit investigations are made available to the Intelligence Services Commissioner for scrutiny.

154. Staff within each Agency are also required to keep their senior leadership *"apprised as appropriate of the relevant Service's bulk personal data holdings and operations."* (§8.5)

Oversight

155. The BPD Handling Arrangements also set out provisions in relation to the oversight of BPD.

156. §9.1 concerns Ministerial oversight. Each of the Intelligence Services must report as appropriate on its BPD holdings and operations to the relevant Secretary of State.

157. §§10.1 to 10.4 address oversight by the Intelligence Services Commissioner:

*"10.1 The acquisition, use, retention and disclosure of bulk personal datasets by the Intelligence Services, and the management controls and safeguards against misuse they put in place, will be overseen by the Intelligence Services Commissioner on a regular six-monthly basis, or as may be otherwise agreed between the Commissioner and the relevant Intelligence Service, except where the oversight of such data already falls within the statutory remit of the Interception of Communications Commissioner.*

***Note**: The Prime Minister's section 59A RIPA direction was issued on 11 March 2015. Paragraph 3 of this makes it clear that the Commissioner's oversight extends not only to the practical operation of the Arrangements, but also to the adequacy of the Arrangements themselves.*

*10.2 The Intelligence Services must ensure that they can demonstrate to the appropriate Commissioner that proper judgements have been made on the necessity and proportionality of acquisition, use, disclosure and retention of bulk personal datasets. In particular, the Intelligence Services should ensure that they can establish to the satisfaction of the appropriate Commissioner that their policies and procedures in this area (a) are sound and provide adequate safeguards against misuse and (b) are strictly complied with, including through the operation of adequate protective monitoring arrangements.*

*10.3 The Intelligence Services Commissioner also has oversight of controls to prevent and detect misuse of bulk personal data, as outlined in paragraph 8.3 and 8.4 above.*

*10.4 The Intelligence Services must provide to the appropriate Commissioner all such documents and information as the latter may require for the purpose of enabling him to exercise the oversight described in paragraph 10.1 and 10.2 above."*

Internal BPD Handling Arrangements

158. In addition to the published BPD Handling Arrangements, GCHQ, MI5 and SIS have their own internal BPD Handling Arrangements, which were also in force from 4 November 2015. Gisted versions of these are at **[2/GCHQ1/71-80]**, **[1/MI51/101-114]** and **[2/SIS/65-78]** respectively. These reflect and supplement the published BPD Handling Arrangements. They are not separately set out in detail here.

GCHQ Compliance Guide

159. The relevant sections of the GCHQ Compliance Guide have been set out above in the section dealing with the position prior to 4 November 2015: see the references to the Compliance Guide from June 2014 onwards: see §§78-83 above.

MI5 internal arrangements

160. MI5 continues to have internal guidance in addition to the BPD Handling Arrangements. In particular:

(a) In November 2015 MI5 updated its internal BPD Guidance **[1/MI51/47-66**]. That sits alongside the internal MI5 Handling Arrangements **[1/MI51/101-114**].

(b) An MI5-specific version of the SIA BPD Policy was used from November 2015 **[1/MI51/67-82**].

(c) A new version of the Form for Retention began to be used in May 2016 **[1/MI51/803-807**].

SIS internal arrangements

161. SIS also continued to have additional internal arrangements: see §§126-127 above.