APPENDIX A: THE SECTION 94 REGIME

1. The regime in respect of section 94 of the Telecommunications Act 1984 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) Section 94 of the Telecommunications Act 1984 [**Auths/ tab 1**];

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

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

   (f) 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 and Security Committee and the Tribunal (see **pages 7-11** below).

3. In addition, GCHQ and MI5 have a number of **internal arrangements** in relation to Section 94; an open summary of which appears at this Appendix (see **pages 12-29** below).

4. In addition:

   (a) MI5 has, as a matter of practice and policy, applied the procedures and safeguards contained in the **Acquisition and Disclosure of Communications Data Codes of Practice** 2007 and 2015 [**Auths/tabs 67 and 75**] to its access to Bulk Communications Data obtained under Section 94 of the Telecommunications Act 1984 (see **pages 30-31** below).

   (b) GCHQ has throughout the periods under consideration as a matter of policy applied the appropriate safeguards set out in the Interception of Communications Code of Practice 2002 and, subsequently, the Interception of Communications Code of Practice 2016 [**Auths/tabs 64, 76**], to all operational data, including BCD obtained under s.94 directions (see **page 31** below).

The SSA and ISA

Security Service functions

5. 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."

6. 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;…"

GCHQ functions

7. 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 ...."

8. 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."

9. 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 ..."

10. 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]

11. 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."*

12. 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."*

13. 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 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))

14. 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)."

15. 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)."

16. 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.

Section 94 of the Telecommunications Act 1984 [Auths/tab 1]

17. S.94 of the Telecommunications Act 1984 ("TA") provides:

    *"**94.- Directions in the interests of national security etc.***

    (1) The Secretary of State may, after consultation with a person to whom this section applies,

give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.

(2) If it appears to the Secretary of State to be necessary to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.

(2A) The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.

(3) A person to whom this section applies shall give effect to any direction given to him by the Secretary of State under this section notwithstanding any other duty imposed on him by or under Part 1 or Chapter 1 of Part 2 of the Communications Act 2003 and, in the case of a direction to a provider of a public electronic communications network, notwithstanding that it relates to him in a capacity other than as the provider of such a network.

(4) The Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.

(5) A person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that the Secretary of State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.

(6) The Secretary of State may, with the approval of the Treasury, make grants to providers of public electronic communications networks for the purposes of defraying or contributing towards any losses they may sustain by reason of compliance with the directions given under this section.

(7) There shall be paid out of money provided by Parliament any sums required by the Secretary of State for making grants under this section.

(8) This section applies to OFCOM and to providers of public electronic communications networks."

18. The Secretary of State's power to give directions under section 94, whether of a general character (s.94(1)) or requiring specific action (s.94(2)) is limited to directions which appear to the Secretary of State to be *"necessary"* in the interests of national security or international relations (s.94(1)) and which the Secretary of State believes to be *"proportionate"* to what is sought to be achieved. The Secretary of State must also first consult with the person to whom the direction is to be given (s.94(1) and (2)).

The HRA [Auths/tab 6]

19. 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*."

20. By s. 6(1):

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

21. 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 bulk activity relating to and section 94 of the Telecommunications Act 1984, the HRA applies at every stage of the process i.e. authorisation/acquisition, use/access, disclosure, retention and deletion.

22. 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**]

23. 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."*

24. 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.

25. 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 <u>not</u> 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]

26. 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]

27. 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).

28. 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

[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.

OSA).

Oversight mechanisms

29. There are three principal oversight mechanisms in respect of section 94 of the Telecommunications Act 1984:

    (a) The Interception of Communications Commissioner;

    (b) The ISC; and

    (c) The Tribunal.

The Interception of Communications Commissioner

30. The Prime Minister must also appoint an Interception of Communications Commissioner (see s. 57(1) of RIPA [**Auths/tab 7**]). 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. The Interception Commissioner has provided oversight over section 94 at both MI5 and GCHQ.

39. At **MI5**, the Commissioner (Sir Paul Kennedy, Sir Anthony May and, most recently IOCCO inspectors on his behalf) has overseen samples of requests for authorisation for access to the database and the related authorisations.

40. In January 2015 the Prime Minister asks Sir Anthony May to extend his oversight of MI5's database capability. In particular, it was agreed that Sir Anthony May's oversight would be extended to cover the issuing, by the Secretary of State, of the section 94 directions and of MI5's storage and destruction arrangements for the data.

41. At **GCHQ**, external oversight over section 94 directions was conducted by Sir Swinton Thomas, the Interception of Communications Commissioner, between 2004 and 2006, and by the Intelligence Services Commissioner (Sir Peter Gibson, and subsequently Sir Mark Waller) between 2006 and 2015.

42. Although not provided on express, agreed, terms, as a matter of practice in advance of each inspection visit the Commissioner was provided with a list setting out details of all the extant s.94 Directions and any that had been cancelled since the previous inspection. On the basis of the list the Commissioner selected one or more Directions. During the visit the Commissioner examined the relevant Direction or Directions, the applications to the Secretary of State for those Directions (which included the necessity and proportionality justifications), and the correspondence with the organisations on whom the Directions were served. Sessions were scheduled to give him the opportunity to question those members of GCHQ involved in applying for the relevant Direction or Directions, those responsible for putting them into effect, and analysts who made use of the data obtained under them. The Commissioner was also provided with information on the extent to which s.94 data contributed to intelligence reporting.

43. As far as the *use* of section 94 data was concerned, it is relevant to note that BCD

obtained by means of section 94 is and was held by GCHQ alongside communications data obtained by means of interception under a section 8(4) warrant. Use of the *combined* data fell to be overseen by the Interception of Communications Commissioner. In addition, the Intelligence Services Commissioner considered the safeguards put in place to identify and address potential abuse of GCHQ's systems. Those systems included, but were not restricted to, those holding section 94 data.

44. As in the case of MI5, in January 2015 the Prime Minister wrote to the Interception Commissioner to ask him to extend his oversight to section 94 BCD directions.

45. 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*."

46. 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).

47. 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

48. 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.

49. 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]**.

50. 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.

---

[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 [**Auths/tab 3**]).

[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 [**Auths/tab 4**]).

51. 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.

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

53. 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.

54. 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.

55. 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.

56. 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

57. 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).

58. The Tribunal's jurisdiction is broad. As regards the Section 94 regimes, 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).

59. 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)).

60. 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.

61. 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.

62. 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.

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

64. 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.

Internal handling arrangements

65. This section addresses the internal handling arrangements in place at GCHQ and MI5 from June 2005 onwards in relation to BCD obtained by section 94 directions. It does so by reference to the periods:

(a) Prior to the avowal of the use of section 94 to obtain communications data and the publication of the section 94 handling arrangements on 4 November 2015 (see **pages 12-22** below);

(b) From 4 November 2015 to the date of the hearing; and

(c) As at the date of the hearing.

((b) and (c) are addressed together at **pages 22-29** below).

a. Prior to the avowal of the use of section 94 to obtain communications data and the publication of the section 94 handling arrangements on 4 November 2015

i. GCHQ

66. In this period, GCHQ's internal 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

67. 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 **[2/GCHQ1/150, 156]**; and for the period June 2014 to 4 November 2015, see **[2/GCHQ1/5, 7, 13, 18]**. For example, in the "Authorisation" section of the Compliance Guide for the periods August 2012 to May 2014 at **[2/GCHQ1/150]**:

"***Direction under s.94 of the Telecommunications Act***

A Direction under s.94 of the Telecommunications Act may be issued by the Secretary of State and served upon a CSP. The Direction cannot direct the CSP to disclose communications content; it can, however, direct the CSP to disclose other information i.e. communications data in the interests of national security and where SoS judges it proportionate..."

See also the identical wording on **[2/GCHQ1/7-8]** for the period June 2014 onwards, which also 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."

Access

68. 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: §67(a) above.

(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]**)

(c) Further, in relation to **reporting** on communications data:

"11. ... full justification and proportionality criteria must be observed when reporting the output." **[2/GCHQ1/106**]

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

(a) In the "Analysis" section at **[2/GCHQ1/147**]:

"...It is GCHQ policy to apply the same legal and policy handling rules to all operational data, whether it is acquired by an 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 operational purposes...*

and

- *proportionate*

To demonstrate the necessity and proportionality of your search, you must supply a HRA justification. This consists of three parts:

- *Purpose and JIC Priority eg 1NS*
- *<u>Requirement</u> 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.*

Your HRA justification should provide enough information about the individual or

organisation so that an uninformed observer e.g. an auditor can understand why it is necessary and proportionate to intrude on an individual's right to privacy..."

(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."*

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

(a) The "Collection and data acquisition" section made clear in respect of, inter alia, *"communications data acquired under Telecommunications Act s.94 directions"* that:

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

(b) Further, 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]**

(c) The "Safeguards" section also stated that *"reporting and other release of Sigint must be necessary and proportionate"* **[2/GCHQ1/156]**

(d) 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]** and Safeguards **[2/GCHQ1/18]** sections.

Disclosure

71. 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 intentions 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**].

Retention/Review/Destruction

72. 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]**

73. In relation to destruction, as already noted, GCHQ treats communications data acquired under section 94 directions 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]**.

ii. Security Service

Access/use

74. From 31 March 2006 (prior to the database becoming operational and functional in May 2006: MI5 statement [**Core/B/2**], §120) onwards internal guidance was in place in relation to authorisation of access to the database [**1/MI51/265-266**]. The guidance, which was headed ("*The database* – Necessity and Proportionality"):

    (a) Emphasised (in §2) that "Access to *the database* data may constitute an interference with individuals' right to privacy."

    (b) Made clear that accordingly access was to be authorised in the same way as access is authorised under Part I Chapter II of RIPA. Analysts were thus required to seek RIPA authorisations (*ibid*.)

    (c) The analyst would have to include a *"persuasive description of the National Security context for each query."* and to provide the Designated Person with *"sufficient information"* to make an *"informed decision"* as to whether or not to authorise (*ibid*.)

    (d) Specifically this meant demonstrating:

        (a) Necessity (*"i.e. that it is valuable intelligence really needed to progress an investigation"*); and

        (b) Proportionality (*"You must also demonstrate that what you will need to do to reach that end state, in terms of the amount of other data you need to access and analyse (and any interference with privacy that entails) is proportionate to the value of the intelligence you seek."*)

    (e) Gave more detailed guidance, including worked examples [**1/MI51/266**].

75. Further internal Security Service guidance for use of the database used for bulk communications data was issued in November 2006 [**1/MI51/267**]. The gist of that guidance which has been disclosed notes (again) that retrieval from the database would be authorised under Part 1 Chapter II of RIPA, and that access would be subject to restrictions.

76. More specific guidance was also issued.

    (a) On 21 January 2008 guidance concerning "out of hours" requests for verbal authorisations to access BCD was issued (*"the person requesting must first speak to a manager to describe the request so that he/she can assess the collateral intrusion and the necessity and proportionality of obtaining the data…verbal authorisation must be obtained before the request is then made."* [**1/MI51/271**])

    (b) In November 2010 a minute was circulated containing revised procedures for authorisation of access to the BCD database by a particular section of the

Security Service. These were *"designed to ensure a clear audit trail."* [**1/MI51/273**])

77. The Security Service held workshops for staff in relation to access to the database: see briefing notes of 24 July 2007 [**1/MI51/269**] and 8 December 2011 (which included reminding analysts that data should only be requested *"for time periods of interest"* [**1/MI51/275**]).

78. In February 2011 the guidance in relation to Communications Data was revised [**1/MI51/-283**]. The *"Communications Data – Guidance on Justifications"* aimed to provide *"applicants for Communications Data with the necessary information to draft justifications which effectively address both necessity and proportionality issues and for DP's [Designated Persons] to identify justifications that are incomplete."* Key sections of the guidance are set out in the MI5 statement [**Core/B/2**], at §§125-127. In particular, the guidance:

(a) Made clear that that core matters for consideration in any request for CD are "necessity, proportionality and intrusion (both collateral and intended intrusion)." [**1/MI51/280**]

(b) Gave detailed guidance as to the meaning of

(a) "Necessity" [**1/MI51/281**]:

"Necessity can be divided into three main points that need to be considered in any communications data justification:
– Background to the investigation – what is that we are investigating?
– What is the subject of the communications data request's relation to the investigation?
– How does the communications address that we are making the request for relate to the target and the investigation?
The applicant must be able to link these three points together in order to demonstrate that any request for communications data is necessary for the statutory purpose specified."

(b) "Proportionality – General":

"When considering proportionality, applicants need to outline how obtaining the data will benefit the investigation and what intrusion into privacy the request will result in. The main things that need to be considered are:
– What are you looking for in the data to be acquired?
– If the data contains what you are looking for, how will this assist you in taking the investigation forward?
– What will be the intrusion into the privacy of the target of the request? Will there be any other intended intrusion taking place?
– Is there another, less intrusive way of obtaining the information you need?
– If a time period of data has been specified, why is this particular time period required e.g. why would a shorter time period not be sufficient?

Therefore, the applicant should explain how the communications data will be used once obtained and how this will benefit the investigation. It is also important that intrusion into the target of the request's privacy is considered.

These points form a large part of the proportionality argument, the other part being in relation to collateral intrusion."

(c) "Proportionality – Collateral Intrusion":

"The key question to be asked in relation to this is:
– Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for? How will this be mitigated?
– If a time period of data has been specified, how will this impact on the identified collateral intrusion?"

79. Guidance was also given to the Designated Person at [**1/MI51/283**]. This included that they should check, with regard to the guidance set out above:

(a) that "*the justification provided by the applicant is sufficient to satisfy the DP that obtaining the requested data is both necessary and proportionate*". Designated Persons are specifically "*required to reject*" any application where they are "*not convinced of both the necessity and proportionality of the request*".

(b) that the intrusion into privacy that will result from the request has been addressed and "*where identified, measures to mitigate collateral intrusion have been outlined*".

(c) that the time period of data requested is proportionate and properly explained and justified.

80. Examples of justifications were given [**1/MI51/283**].

81. This guidance has been amended on several occasions: see MI5 statement [**Core/B/2**], §124, and **1/MI51/285-304** and **115-152**. The subsequent versions were essentially identical, albeit with some minor changes of phrasing, and save that:

(a) From January 2012 [**1/MI51/285-290**] onwards the guidance explained the National Priority Grading System (NPGS) detailed in the Communications Data Code of Practice, which categorised requests for communications data as Very Urgent, Urgent and Routine.

(b) From November 2013 [**1/MI51/115-118**] onwards more guidance was given as to the term "*meaningful collateral intrusion*":

" "Meaningful collateral intrusion" includes collateral intrusion that we can foresee is "highly likely" – such as family members using the landline or internet connection where they live. However, we should not speculate where possible collateral intrusion cannot be said to be "highly likely"…"

82. The guidance has remained in force since avowal of Section 94 BCD in November 2015. It is addressed at §111 below.

83. Further guidance for investigators making requests for communications data was created in September 2011 [**1/MI51/153**], and again in August 2014 [**1/MI51/155**]. The latter document (which is still in force) noted:

"Key to meeting our legal obligations is being proportionate, i.e. only obtaining the minimum amount of data required to achieve our objective (an objective which should be necessary in the interests of national security)

CRD is an intrusive investigative tool: investigators should make a judgment as to which request is proportionate based upon the individual case. Consider whether, in the context of operational requirements, an incremental approach to obtaining the data needed should be used."

84. On 22 May 2013 advice was circulated for those authorising bulk communications data requests [**1/MI51/277**]. Authorising officers were particularly directed to take account of the intelligence background, collateral intrusion and the need for data and its proposed use.

85. In April 2015 guidance was produced (**1/MI51/157**) for Designated Persons for implementing the new Acquisition and Disclosure of Communications Data Code 2015 (as to which see §§115-116 below).

Retention/review/destruction

86. The appropriate retention period was initially six months, before being revised upwards, and then fixed in November 2009 at one year. Any data that is older than one year is automatically deleted [**Core/B/2/MI5 statement, §130**].

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

87. The Section 94 Handling Arrangements, which came into force on 4 November 2015 [**2/GCHQ1/195-204**], apply to bulk communications data obtained under section 94 of the Telecommunications Act 1984. They are mandatory and required to be followed by staff in the Intelligence Services. Failure to comply may lead to disciplinary action, which can include dismissal and prosecution (§§1.1-1.3).

88. The Section 94 Handling Arrangements expressly relate to communications data which is limited to "traffic data" and "service use information" (§2.2). These terms are defined at §3.5.1 and §3.5.2 by reference to s.21(4) and (6) of RIPA:

"3.5.1 ***Section 21(4)*** *of* ***RIPA*** *defines 'communications data' as meaning any of the following:*

- ***Traffic Data*** *– this is data that is or has been comprised in or attached to a communication for the purpose of its transmission [section 21(4)(a)];*
- ***Service Use Information*** *– this is the data relating to the use made by a person of a communications service [section 21(4)(b)];*

..."

3.5.2 ***Section 21(6)*** *defines 'traffic data' for these purposes, in relation to any communication, as meaning:*

- *any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted;*

- *any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted;*

- *any data comprising signals for the actuation of apparatus used for the purposes of a telecommunications system for effecting (in whole or in part) the transmission of any communication; and*

- *any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored."*

89. The data provided does <u>not</u> contain communication content or Subscriber Information or Internet Connection Records (§2.3). Subscriber Information is defined at §3.5.1:

"***Subscriber Information*** *– this relates to information held or obtained by a communications service provider about persons to whom the communications service provider provides or has provided communications services [section 21(4)(c)]."*

90. §2.4 sets out the requirements contained in section 94 itself that the Secretary of State must be satisfied that a Section 94 direction is **necessary** and **proportionate**:

"2.4 Any section 94 Directions under which this communications data is acquired requires the relevant Secretary of State to be satisfied that acquisition is necessary in the interests of national security or international relations and that the level of interference with privacy involved in doing so is proportionate to what it seeks to achieve."

91. The requirement that acquisition, use, retention and disclosure of BCD have "*clear justification, accompanied by detailed and comprehensive safeguards against misuse*" and be "*subject to rigorous oversight*" is made clear (§4.0.1). The Section 94 Handling Arrangements are intended to provide such safeguards (§4.0.2).

92. The Section 94 Handling Arrangements set out provisions in respect of each of the stages of the lifecycle of BCD.

<u>Acquisition</u>

93. §§4.1.1-4.1.2 sets out the key considerations which must be presented to the Secretary of State when he/she considers whether to make a Section 94 Direction. These include the family considerations of necessity and proportionality, including whether a less intrusive method of obtaining the information is available, and the level of collateral intrusion involved:

"4.1.1 Where the head of the relevant Intelligence Service has decided to request a Section 94 Direction from the relevant Secretary of State, it is essential that a submission is then presented to the Secretary of State by the Home Office/Foreign Office in order to enable them to consider:

- *whether acquisition and retention of the BCD to be authorised by the Direction is necessary in the interests of national security or international relations;*
- *whether the acquisition and retention of the BCD would be proportionate to what is sought to be achieved;*
- *whether there is a less intrusive method of obtaining the BCD or achieving the national security objective;*
- *the level of collateral intrusion caused by acquiring and utilising the requested BCD.*

4.1.2 The submission must also outline any national security or international relations argument as to why the Secretary of State cannot lay the Direction before each House of Parliament in accordance with 94(4) of the Act."

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

"When will acquisition be "necessary"?

*4.1.3 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, before presenting the submission referred to in paragraph 4.1.1 above, staff in the relevant Intelligence Service must consider why obtaining the BCD in question is 'really needed' for the purpose of discharging a statutory function of that 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"

*4.1.4 The obtaining and retention of the bulk communications dataset must also be **proportionate** to the purpose in question. In order to meet the '**proportionality**' requirement, before presenting the submission referred to in paragraph 4.1.1 above, staff in the relevant Intelligence Service must balance (a) the level of interference with the right to privacy of individuals whose communications data is being obtained (albeit that at the point of initial acquisition of the BCD the identity of the individuals will be unknown), both in relation to subjects of intelligence interest and in relation to other individuals 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."*

95. Once made, a Section 94 Direction must be served on the CNP concerned in order that the relevant Agency can receive the requested dataset (§4.2.1).

96. Safeguards against unauthorised access are set out at §4.2.2:

"4.2.2 It is essential that any BCD is acquired in a safe and secure manner and that Intelligence Services safeguard against unauthorised access. Intelligence Services must therefore adhere to the controls outlined in the CESG[6] Good Practice Guide for transferring and storage of data electronically or physically."

Access/use

97. The Section 94 Handling Arrangements emphasise the importance of data security and protective security standards, confidentiality of data and preventing/disciplining misuse of such data:

"4.3.1 Each Intelligence Service must attach 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 BCD 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."

98. As with BPD, 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:

"*4.3.2 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.*

4.3.3 Furthermore, each Intelligence Service is obliged to put in place the following additional measures:

- *Access to BCD must be strictly limited to those with an appropriate business requirement to use these data and managed by a strict authorisation process;*
- *Requests to access BCD must be justified on the grounds of **necessity** and **proportionality** and must demonstrate consideration of collateral intrusion and the use of any other less intrusive means of achieving the desired intelligence dividend.*
- *Intelligence Service staff who apply to access BCD must have regard to the further guidance on the application of the **necessity** and **proportionality** tests set out in paragraph 4.1.3 - 4.1.4 above.*
- *Where Intelligence Service staff intend to access BCD relating to the communications of an individual known to be a member of a profession that handles privileged information*

[6] UK Government's National Technical Authority for Information Assurance.

or information that is otherwise confidential (medical doctors, lawyers, journalists, Members of Parliament, Ministers of religion), they must give ***special consideration*** *to the necessity and proportionality justification for the interference with privacy that will be involved;*

- *In addition, Intelligence Service staff must take particular care when deciding whether to seek access to BCD and must consider whether there might be unintended consequences of such access to BCD and whether the public interest is best served by seeking such access;*
- *In all cases where Intelligence Service staff intentionally seek to access and retain BCD relating to the communications of individuals known to be members of the professions referred to above, they must record the fact that such communications data has been accessed and retained and must flag this to the Interception of Communications Commissioner at the next inspection;*
- *In the exceptional event that Intelligence Service staff were to seek access to BCD specifically in order to determine a journalist's source, they should only do this if the proposal had been approved beforehand at Director level. Any communications data obtained and retained as a result of such access must be reported to the Interception of Communications Commissioner at the next inspection;*
- *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 BCD 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;*
- *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.*
- *In the exceptional event that Intelligence Service staff were to abuse their access to BCD – for example, by seeking to access the communications data of an individual without a valid business need – the relevant Intelligence Service must report the incident to the Interception of Communications Commissioner at the next inspection."*

Disclosure

99. The disclosure of BCD outside the Agency which holds can only occur if certain conditions are complied with:

"4.4.1 The disclosure of BCD must be carefully managed to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The disclosure of an entire bulk communications dataset, or a subset, outside the Intelligence Service may only be authorised by a Senior Official[7] or the Secretary of State.

4.4.2 Disclosure of individual items of BCD outside the relevant Intelligence Service may only be made if the following conditions are met:

[7] Equivalent to a member of the Senior Civil Service.

- *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."*

100. Again, guidance is given to staff on the requirements of **necessity** and **proportionality**, in terms similar to those relating to acquisition, but with specific reference to disclosure:

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

*4.4.3 In order to meet the '**necessity**' requirement in relation to disclosure, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that disclosure of the BCD is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.*

The disclosure must also be "proportionate"

*4.4.4 The disclosure of the BCD must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that the level of interference with the right to privacy of individuals whose communications data is being disclosed, both in relation to subjects of intelligence interest and in relation to other individuals who may be of no intelligence interest, 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 communications data or of a subset of the bulk communications data rather than of the whole bulk communications dataset."*

101. Prior to any disclosure of BCD, 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 (§4.4.5). This applies to all disclosure, including to other Agencies (§4.4.6), and whether disclosure is of an entire BCD, a subset of a BCD or an individual piece of data from a BCD (§4.4.6).

102. Disclosure of the whole or subset of a BCD may only be authorised by a Senior Official (equivalent to a member of the Senior Civil Service) or the Secretary of State (§4.4.1).

<u>Retention/review/deletion</u>

103. The requirement on each of the Intelligence Services to review the justification for continued retention and use of BCD is set out at §§4.5.1-4.5.2:

"4.5.1 Each Intelligence Service must regularly review, i.e. at intervals of no less than six months, the operational and legal justification for its continued retention and use of BCD. This should be managed through a review panel comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams.

4.5.2 The retention and review process requires consideration of:

- *An assessment of the value and use of the dataset during the period under review and in a historical context;*
- *the operational and legal justification for ongoing acquisition, continued retention, including its necessity and proportionality;*
- *The extent of use and specific examples to illustrate the benefits;*
- *The level of actual and collateral intrusion posed by retention and exploitation;*
- *The extent of corporate, legal, reputational or political risk;*
- *Whether such information could be acquired elsewhere through less intrusive means.*

4.5.3 Should the review process find that there remains an ongoing case for acquiring and retaining BCD, a formal review will be submitted at intervals of no less than six months for consideration by the relevant Secretary of State. In the event that the Intelligence Service or Secretary of State no longer deem it to be necessary and proportionate to acquire and retain the BCD, the Secretary of State will cancel the relevant Section 94 Direction and instruct the CNP concerned to cease supply. The relevant Intelligence Service must then task the technical team[s] responsible for Retention and Deletion with a view to ensuring that any retained data is destroyed and notify the Interception of Communications Commissioner accordingly. Confirmation of completed deletion must be recorded with the relevant Information Governance/Compliance team."

Oversight

104. The Section 94 Handling Arrangements also set out provisions in relation to internal and external oversight.

105. §§4.6.1-4.6.2 concern internal oversight. A senior member of an Intelligence Service's internal review panel (see §106 above) must keep that Service's Executive Board apprised of BCD holdings (§4.6.1). In addition internal audit teams must monitor use of IT systems:

"4.6.2 Use of IT systems is monitored by the audit team 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. Disciplinary action may be taken, which in the most serious cases could lead to dismissal and/or the possibility of prosecution under the Computer Misuse Act 1990, the Data Protection Act 1998, the Official Secrets Act 1989 and Misfeasance in Public Office depending on circumstances."

106. All reports on audit investigations are made available to the Interception of Communications Commissioner (§4.6.3).

107. §§4.6.4 to 4.6.7 address oversight by the Interception of Communications Commissioner:

*"4.6.4 The **Interception of Communications Commissioner** has oversight of:*

a) the issue of Section 94 Directions by the Secretary of State enabling the Intelligence Services to acquire BCD;

b) the Intelligence Services' arrangements in respect of acquisition, storage, access, disclosure, retention and destruction; and

c) the management controls and safeguards against misuse which the Intelligence Services have put in place.

4.6.5 This oversight is exercised by the Interception of Communications Commissioner on at least an annual basis, or as may be otherwise agreed between the Commissioner and the relevant Intelligence Service.

4.6.6 The purpose of this oversight is to review and test judgements made by the Secretary of State and the Intelligence Services on the necessity and proportionality of the Section 94 Directions and on the Intelligence Services' acquisition and use of BCD, and to ensure that the Intelligence Services' policies and procedures for the control of, and access to BCD are (a) are sound and provide adequate safeguards against misuse and (b) are strictly observed.

4.6.7 The Interception of Communications Commissioner also has oversight of controls to prevent and detect misuse of data acquired under Section 94, as outlined in paragraph 4.6.2 and 4.6.3 above."

108. The Secretary of State and the Intelligence Services must provide the Interception of Communications Commissioner with *"all such documents and information as he may require for the purpose of enabling him to exercise the oversight described…"* (§4.6.8)

Internal Section 94 Handling Arrangements

109. In addition to the published Section 94 Handling Arrangements, both GCHQ and MI5 have their own internal Section 94 Handling Arrangements, which were also in force from 4 November 2015. Gisted versions of these are at **2/GCHQ1/71-88** and **1/MI51/163-175** respectively. These reflect and supplement the published Section 94 Handling Arrangements. They are not separately set out in detail here.

GCHQ Compliance Guide

110. 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 at §§67-73 above.

MI5 internal arrangements

111. MI5 continues to have internal guidance in addition to the Section 94 Handling

Arrangements. In particular:

(a) From November 2015 the "Communications Data – Guidance on Justifications and Priorities" guidance [**1/MI51/133-142**] was amended so that:

  (a) Specific attention was drawn (and a link provided to) the MI5 Section 94 Handling Arrangements which came into force on 4 November 2015; and

  (b) Detailed guidance was provided in respect of communications data applications relating to members of sensitive professions.

Acquisition and Disclosure of Communications Data Codes of Practice

112. As noted at §131 of the MI5 statement [**Core/B/2**], the authorisation process for access to the Section 94 database was, from the outset, the same as for requests to CSPs for CD under Part 1 Chapter II of RIPA. As a matter of practice and policy, MI5 has applied the applicable Codes of Conduct for the acquisition of communications data to the regime that it has operated for the database. In particular, investigators would – when completing requests for CD – be expected to comply with applicable parts of the Code of Practice relating to the acquisition of CD.

Acquisition and Disclosure of Communications Data Code of Practice 2007 [Auths/tab 67]

113. The Acquisition and Disclosure of Communications Data Code of Practice 2007 ("the 2007 CD Code") related to the powers and duties conferred under Part 1 Chapter II of RIPA [**Auths/tab 7**].

114. Relevant provisions of the 2007 CD Code include:

(a) Provisions emphasising and explaining the requirements of necessity and proportionality:

(a) *"The acquisition of communications data under the Act will be a justifiable interference with an individual's human rights under Article 8 of the European Convention on Human Rights only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law."* (§2.1)

(b) *"Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation. An application for the acquisition of communications data should draw attention to any circumstances which give rise to a meaningful degree of collateral intrusion."* (§2.6)

(c) Further explanation of proportionality at §§2.7-2.8.

(b) The procedure for making an application: at §§3.3-3.6, §§3.56-3.62.

(c) The role of "Designated Persons":

(a) *"Exercise of the powers in the Act to acquire communications data is restricted to designated persons in relevant public authorities. A designated person is someone holding a prescribed office, rank or position with a relevant public authority that has been designated for the purpose of acquiring communications data by order."* (§2.9)

(b) *"The designated person must believe that the conduct required by any authorisation or notice is necessary. He or she must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the intrusiveness of the*

interference with an individual's right of respect for their private life against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest" (§2.5) Further details were given at §§3.7-3.14.

(d) Provisions concerning disclosure, handling and storage of communications data: Chapter 7.

Acquisition and Disclosure of Communications Data Code of Practice 2015 [Auths/tab 75]

115. The Acquisition and Disclosure of Communications Data Code of Practice of March 2015 ("the 2015 CD Code") contained similar provisions as to:

(a) Necessity and proportionality: see §2.1; §§2.6-2.9. However, more detailed guidance on necessity and proportionality was given at §§2.36-2.45.

(b) The procedure for making an application: §§3.3-3.6.

(c) Designated Persons: §2.10; §3.7ff.

(d) Disclosure, handling and storage of communications data: Chapter 7.

116. Guidance was also given in the 2015 CD Code about Communications Data involving specified professions: §3.72-§3.84.

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

117. GCHQ has throughout the periods under consideration as a matter of policy applied the appropriate safeguards set out in the Interception of Communications Code of Practice 2002 and, subsequently, the Interception of Communications Code of Practice 2016, to all operational data, including BCD obtained under s.94 directions. Those Codes of Practice included provisions as to:

(a) **Necessity** and **proportionality** in relation to

(a) Applications for and the granting of 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.

(b) Renewal/cancellation of 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 material (**2002 Code**, §6.2, §6.4; **2016 Code**, §7.3, §7.5-§7.6, §7.9); storage (**2002 Code**, §6.7, §7.7); and destruction (**2002 Code**, §6.8, §7.8).