Neutral Citation Number: [2018] UKIPTrib IPT_15_110_CH

No: IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

P.O. Box 33220
London
SW1H 9ZQ

23rd July 2018

SIR MICHAEL BURTON (PRESIDENT)
THE HON. MR. JUSTICE EDIS
SIR RICHARD MCLAUGHLIN
MR. CHARLES FLINT QC
MS. SUSAN O'BRIEN QC

- -

Between:

PRIVACY INTERNATIONAL	**Claimant**
- and -	
(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS **(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT** **(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS** **(4) SECURITY SERVICE** **(5) SECRET INTELLIGENCE SERVICE**	**Respondents**

- -

Mr T De La Mare QC, Mr B Jaffey QC and **Mr D Cashman** (instructed by **Bhatt Murphy Solicitors**) appeared on behalf of the **Claimant**

Sir James Eadie QC, Mr A O'Connor QC and **Mr R O'Brien** (instructed by **Government Legal Department**) appeared on behalf of the **Respondents**

Mr J Glasson QC (instructed by **Government Legal Department**) appeared as **Counsel to the Tribunal**

Hearing dates: 17, 18 and 19 October 2017, 1 December 2017, 10 January 2018, 26 February 2018 and 12 -13 March 2018.

- -

JUDGMENT

Sir Michael Burton (President):

1. This is the Judgment of the Tribunal, to which all its members have contributed.

2. From our Judgment of 17 October 2016 ("the First Judgment"), the first issue which remained outstanding for resolution was addressed by our Judgment dated 8 September 2017 (with a postscript of 11 September 2017) ("the Second Judgment"), namely the compatibility of the collection, retention and use of bulk communications data with EU law, and we made a Request for Preliminary Ruling by a Reference to the CJEU in relation to that Judgment on 18 October 2017. Unless freshly defined or redefined in this Judgment, we shall use the same terms or abbreviations as we used in those Judgments.

3. There were then the following issues remaining for resolution:-

   (i) S.94 of the Telecommunications Act 1984 ("s.94") relating to the obtaining of BCD, pursuant to directions given under that Act. This issue was expressed as whether there had been unlawful delegation of the statutory powers of the Foreign Secretary under s.94, but it has been expanded so as to include whether the directions given by the Foreign Secretary under s.94 complied with the terms of his statutory duty or were in accordance with the law ("Issue 1").

   (ii) What is the consequence of the finding of unlawfulness we made in the First Judgment in respect of the BCD regime prior to 4 November 2015 (resulting from our finding that there was contravention of Article 8 of the ECHR), now extended to cover the consequences of any conclusion made in respect of Issue 1 ("Issue 2")? This is largely consequential on our findings on other Issues, and did not of itself require much consideration of evidence.

(iii) Sharing of BCD/BPD. ("Issue 3") This issue is addressed on the basis of assumptions or hypotheses, a course regularly adopted by this Tribunal, and as further discussed in paragraph 61 below. On the hypothesis that there has been sharing of BCD or BPD, would that be lawful with (a) foreign agencies (at ECHR or EU law) ("Issue 3A"), (b) Law Enforcement Agencies ("LEAs"), such as the Police or HMRC (at ECHR, EU or domestic UK law) ("Issue 3B"), (c) contractors or researchers (called "Industry Partners") (at ECHR or EU law) ("Issue 3C").

(iv) Do the steps taken by way of collection, retention or use of BCD or BPD comply with the requirements of proportionality (there is not suggested to be any different test by reference to the ECHR or EU law) ("Issue 4").

4. In addition, the Claimant made an application to reopen the First Judgment, insofar as it concluded that the oversight by the Commissioners (the Intelligence Services Commissioner) (ISCom) and the Interception of Communications Commissioner (IOCC)) was adequate in respect of BPD subsequent to March 2015 and BCD subsequent to 4 November 2015. We directed that the Claimant had a sufficient case to justify consideration of reopening our Judgment in this regard, at a hearing on 1 December 2017, on the basis that, if we in the event decided by this Judgment to reopen such conclusion, there might need to be the opportunity for fresh evidence to be adduced on that issue, so that it could be decided afresh ("Issue 5").

5. With regard to the above Issues, we needed to consider both open and closed evidence and submissions. Evidence was served additionally to that which we considered for the purposes of our earlier Judgments. This was primarily by the Respondents, both open and closed, including evidence in response to information supplied, at the

Tribunal's request, by the body now substituted for the two separate Commissioners as a result of the Investigatory Powers Act 2016 ("IPA 2016"), namely IPCO (the Investigatory Powers Commissioner's Office). There was some evidence by the Claimants in response to that of the Respondents; and we have heard a representative of GCHQ orally cross-examined in open hearing. Thus there were three days of open hearing between 17 and 19 October 2017 (incorporating a short closed hearing on the third day), the open hearing on 1 December, to which we have referred, a closed hearing to hear closed evidence on 10 January 2018, a closed hearing on 26 February 2018 for the purpose of hearing closed submissions, which was interrupted by the open hearing to cross-examine the witness referred to above and then completed on 12 March, and then closing submissions for the rest of 12 March and on 13 March; there were some written submissions thereafter from the parties and from IPCO. At each stage, but particularly in relation to the closed hearings and the closed evidence, and the substantial opening up of parts of that closed evidence, we were greatly assisted by Jonathan Glasson QC, as Counsel to the Tribunal.

6. It is apparent from the description given in this last paragraph that this has been an iterative exercise, involving substantial consideration of new facts and issues, covering a wide area, and we wish to make a number of general points:-

(i) The dedication and hard work of the Claimant's representatives has been very considerable throughout this exercise, and the Tribunal, the public and indeed the Respondents owe them a debt of gratitude for their patience and perseverance, as well as their considerable and valuable inquisitiveness. It is not irrelevant that this Tribunal is called the Investigatory Powers Tribunal, because, in addition to reaching a number of judicial conclusions, it has been

constantly necessary, in this case in particular, for the Tribunal, at the instance of the Claimant, but very often at the instance and with the assistance of the Counsel to the Tribunal, to probe and to consider fresh problems and lacunae.

(ii) Both for those reasons and because the Tribunal itself is anxious to assist in achieving improvements in the ways in which the Agencies carry out their responsibilities, there has been a constant increase in the amount of information made available to the public, always subject to the need to balance such openness against the needs of national security. As we have said before, it is important not to identify as the discovery of a failing what is, in fact, the identification of a welcome improvement.

(iii) We shall consider later the question of oversight, but that, too, is an iterative process, beginning in this case, as we have described in our First Judgment, with two Commissioners dealing with overlapping remits, and both achieving improvements by percipient identification of problems and discussion of solutions.

(iv) After recognising all of this, and recognising, too, the extremely sensitive area with which we are dealing, which inevitably means that those with responsibilities in those areas may be overcautious in what they feel able to say, we record that, on a number of occasions in the evidence before us, statements by those in a position of responsibility at GCHQ have had to be subsequently corrected. In each case such corrections have been made as a result of re-thinking or double-checking by the witness and his team of some of those issues. It is regrettable that mistakes were made to begin with and not identified earlier, and particularly in relation to Issue 1 the corrected errors

have been influential in our conclusions (see paragraphs 12-15 and 40 below). We have identified in our accompanying CLOSED Judgment five further serious such errors which had been picked up by the Respondents themselves and corrected. To the extent that these errors were also present in information provided to the Commissioners, this will have meant that the Commissioners were not overseeing GCHQ on the basis of a complete and accurate picture of what it was actually doing. We are satisfied that the giving of the incorrect information constituted a breach of GCHQ's duty to make disclosure to the Tribunal under s68(6) of RIPA, but the duty is a continuing one and we accept that the breaches have now been remedied.

7. We turn to consideration of the five issues. There is a CLOSED judgment, to which we have provided an open introduction, which is annexed to this Judgment as Appendix 1.

Issue 1: s.94

8. Following the First Judgment, a declaration was made that prior to 4 November 2015 the regime for the collection of bulk communications data ("BCD") under s.94 Telecommunications Act 1984 did not comply with the law. The further issue now to be decided is whether the directions issued by the Foreign Secretary which required communications service providers ("CSP") to continue to provide BCD to GCHQ after 4 November 2015 were unlawful, on the grounds that the power of direction had been unlawfully delegated to the Director of GCHQ. In the course of submissions that argument was widened to include the issue whether the directions failed to comply with the requirements of necessity and proportionality or were not in accordance with the law. There is no challenge to the legality of the directions issued under s.94 by the

Second Respondent, the Home Secretary, to CSPs requiring production of BCD to the Security Service.

9. S.94, as amended from 25 July 2003, provides as follows:

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 …

10. At 4 November 2015 a number of directions made by the Foreign Secretary between 29 November 2001 and 16 September 2012 remained in force. On 14 October 2016, following receipt by the Respondents of a draft of the First Judgment, the Foreign Secretary made new directions which were intended to replace the existing directions and comply with a recommendation made by the IOCC that directions should indicate the specific communications data that is required to be disclosed. The Claimant also challenges the legality of those new directions, but only on the grounds of unlawful delegation.

11. There is no dispute that s.94 does not permit the Secretary of State to delegate to the Director of GCHQ the power to make a direction, under the principle established in **Carltona v Commissioners of Works** [1943] 2 All ER 560. The main issue in argument was whether the process under which directions made by the Foreign Secretary required the provision of communications data "*if requested to do so by GCHQ*", but the specific data to be required under those directions was determined by GCHQ, amounted to a substantive transfer of the power conferred by s.94 on the Foreign Secretary personally. However, as the argument developed, it became clear that questions of proportionality and whether the directions were made in accordance with the law also required to be considered.

Evidence

12. The Respondents' case on the delegation argument initially asserted that it was the Foreign Secretary, not GCHQ, who made the decision as to which communications data was required to be provided by each CSP. That case was based on the 4th open witness statement of the GCHQ witness dated 16 June 2017, which exhibited at

GCHQ9 and GCHQ10 redacted forms of direction made by the Foreign Secretary. That evidence was very clear in stating that the role of GCHQ officials in making requests for communications data was "*a purely formal one*", as the officials had no discretion as to the categories of data that were to be provided. It was stated that in practice the categories of data to be provided "*are and always have been decided by the Foreign Secretary*". The basis for that statement was that, although the datasets to be provided were not specified on the form of direction used prior to 2016, (a) the datasets to be provided were "*routinely*" set out in the submission to the Foreign Secretary, (b) requests for communications data "*were always made immediately following the making of the direction by the Foreign Secretary*", (c) in the event that GCHQ wished to change the datasets the approval of the Foreign Secretary had to be sought, and (d) no selection or alteration of datasets to be provided "*has ever been made unilaterally by the Director of GCHQ or any other official*". That evidence formed the basis of the Respondents' submissions at paragraphs 62 - 68 of the skeleton argument served on 6 October 2017, which were advanced orally at the hearing held on 17 and 18 October 2017.

13. That evidence was supplemented in the 8th witness statement dated 24 November 2017, which exhibited at GCHQ13 redacted copies of the form of "*trigger letters*" sent by the Director of GCHQ to the CSP. Reference was made to the 4th witness statement as describing the process by which s. 94 directions had been made, without any indication that that evidence might have been inaccurate.

14. On 16 November 2017 the Tribunal requested further details about the process by which s.94 directions were obtained from the Foreign Secretary. On 15 December

2017 the 10th witness statement of the GCHQ witness was served. That statement made a number of substantial corrections to the evidence which had been set out in his 4th witness statement. The witness accepted that in a number of cases the submissions to the Foreign Secretary did not specify the data to be sought from the CSP, the directions were of a general nature and the specific data to be provided were specified by GCHQ in trigger letters or orally. The explanation given for the errors was that the witness had relied on his own knowledge and understanding, and that it was only after the Tribunal had requested further information that further searches had been undertaken to identify the underlying documentation which was then analysed.

15. The Claimant applied for a direction that the GCHQ witness be cross-examined, and that cross-examination took place on 26 February 2018. The explanation of the witness for the errors in his 4th witness statement was that he had not fully read the file of relevant documents but had relied on information from others in GCHQ. That explanation was not entirely consistent with that advanced at paragraph 22 of his 10th witness statement and was surprising, given that the file of all relevant documents had apparently been compiled and made available to the IOCC for the purpose of his review which commenced in October 2015.

16. Following that evidence, the Third Respondent was unable to maintain the general submission that in all or most cases the effect of the direction was that the Foreign Secretary had made a decision specifying the particular communications data which the CSP was required to provide. Instead the argument now put forward is that the Foreign Secretary had power to make a general direction in effect covering all communications data held by the CSP, and to direct that data be provided as requested

by GCHQ. That, it is argued, is a direction which does not involve any delegation to GCHQ even in cases where officials decide which sub-sets of data are to be provided under the direction.

17. The Tribunal has received a substantial volume of closed material which evidences the process under which s.94 directions were made by the Foreign Secretary and acted upon by GCHQ. That material includes submissions made by GCHQ, submissions and notes made by officials within the Foreign Office, directions made, letters requesting data sent by GCHQ to communications providers, and periodic reviews submitted to the Foreign Secretary by GCHQ on the scope and operation of the directions. Those documents comprise all directions made by the Foreign Secretary between 1998 and 2016 relating to communications data.

Facts

18. On the issues, the only relevant directions are those which remained in force as at 4 November 2015 (see paragraphs 22-31 below), and the replacement directions made on 14 October 2016 (see paragraph 37 below). All these directions were made under s.94(1) and required the production of communications data relating to communications through networks operated by the CSPs. A number of directions had been made between 23 March 1998 and 15 March 2001 but none of those directions remained in force on 4 November 2015.

19. During the relevant period the procedure for making directions under s.94 varied to some extent, but in general was as follows:

(a) GCHQ officials would discuss with a CSP what communications data could be provided to meet a current intelligence requirement;

(b) A written submission would be made to the Foreign Secretary, describing in general terms the type of communications data to be sought under the direction, the operational need to obtain such data, how the data would be used and (after 2003) the proportionality of using a direction made under s.94 for these purposes, and the grounds for keeping the direction secret; the submissions noted that the Director of GCHQ would be responsible for reviewing every 6 months the continuing need for the data to be supplied under the directions;

(c) The Foreign Secretary would make a direction in general terms which, in most cases, did not contain any limitation on the category of communications covered by the direction, but required production of data relating to all communications through the specified networks operated by the CSP. The standard form of direction set out the generic type of technical data required, but did not set any limits on the class of communications in respect of which that data was to be provided. The direction required the CSP to provide communications data "*if requested to do so by* [GCHQ]". In that form the direction would have empowered GCHQ to require the production of any communications data from the networks operated by the CSP, not limited to any categories of communications which may have been described in the submission;

(d) In some, but not all, cases a copy of the direction made by the Secretary of State was sent or shown by GCHQ to the CSP;

(e) In some cases a letter, referred to in the evidence as a trigger letter, was sent by GCHQ to the CSP which specified the categories of communications in respect of which data was required by GCHQ. However in most of the relevant cases such letters cannot be found on the files of GCHQ or the CSP. As was accepted by the GCHQ witness, the likelihood is that in such cases the requirement to provide communications data and the specification of such data was communicated only orally.

20. At paragraph 11 of the 10th GCHQ witness statement it is stated that the standard form of directions contained "*a redacted passage which gave more detail of the generic categories of data sought*". That is correct, in that the generic technical type of communications data to be provided was specified, but the directions did not define the categories of communications to which the direction applied. At paragraph 12 of the statement it is stated:

> *"[CSPs] have only ever been asked to provide communications data in respect of particular datasets relating to GCHQ's intelligence requirements. Those datasets were not specified on the old form of direction [ie. the directions made before 14 October 2016]"*.

21. To the extent that it is possible to do so in an open judgment, the facts relating to the relevant directions (i.e. those remaining in force at 4 November 2015 or made on 14 October 2016) are set out below.

22. On 22 November 2001 a submission was made to the Foreign Secretary seeking a number of directions under s.94(1). The submission was made following the attack on the World Trade Centre in New York on 9 September 2001. The operational case for such directions was clearly explained, concluding that GCHQ's ability to obtain and analyse communications data was central to its counter-terrorism work. The submission did not set out which particular types of communications were to be targeted. It made clear that GCHQ was seeking a direction in general terms which would potentially permit it to request data of very wide scope, but stated that:

> *"GCHQ will in practice limit its requests to data that we can be confident is relevant to meeting [JIC] requirements for secret intelligence. GCHQ will consult with the [CSPs] prior to levying any new requirements on them …"*

The submission (and most of the submissions referred to below) included a statement that the Director of GCHQ would be responsible for reviewing every 6 months the continuing need for the data supplied under the direction. The directions made on 29 November 2001 were in general form, covering all communications on any network operated by the CSP to which it was addressed. In some cases trigger letters were issued by GCHQ on 17 January 2002, which specified the particular subsets of data required. The trigger letters stated that the requirement under the direction would lapse after 6 months unless the request was further renewed.

23. When these directions were made on 29 November 2001, s.94 had not been amended to reflect the requirements of the Human Rights Act 2000. S.94 was amended from 25 July 2003 to introduce, inter alia, at s.2A the requirement of proportionality. From 1 April 2003 there was an internal compliance guide produced by GCHQ which set out

in very general terms the Human Rights Act considerations which affected the use of s.94 directions.

24. From July 2004 the IOCC was made aware of the use of s.94 directions and was asked for his advice on some issues. However at that time IOCC did not review any of the directions, nor the submissions made to the Foreign Secretary.

25. On 30 October 2006 a submission was made seeking a further direction. The submission did specify, with reasonable clarity, the type of communications which the direction was intended to cover and clearly set out the necessity for the making of the direction. In respect of safeguards, the submission noted that the communications data would be used only for the purposes specified in s.4(2) of the Intelligence Services Act 1994 ("ISA") and that a compliance document setting out how the data would be handled had been sent to the Foreign Secretary and to the IOCC. A direction was made which, in its particular context, did adequately specify the communications data which was required by GCHQ. The classes of data required by GCHQ were not set out in a trigger letter, but on the evidence the communications data provided were in line with the submission and the direction.

26. On 11 April 2007 a submission was made seeking a further direction. The submission did specify, with reasonable clarity, the type of communications which the direction was intended to cover and clearly set out the necessity for the making of the direction. In respect of safeguards the submission noted that the communications data would be used only for the purposes specified in s.4(2) of ISA and that a compliance document setting out how the data would be handled had been approved by the Foreign

Secretary and reviewed by IOCC. All subsequent submissions seeking directions contained similar text in relation to safeguards. A direction was made on 21 April 2007 which, in its particular context, did adequately specify the communications data which was required by GCHQ. The classes of data required by GCHQ were not set out in a trigger letter but were in line with the submission and the direction.

27. On 11 June 2007 a submission was made seeking a direction in respect of specified parts of the networks operated by a CSP. That submission did specify the type of communications which the direction was intended to cover, and clearly set out the necessity for the making of the direction. The direction made on 21 June 2007 was made in general form applying to all communications through the networks operated by the CSP. The requirements made by GCHQ were set out in a trigger letter and were in line with the submission. The letter also stated that the requirement would lapse in 6 months unless renewed by the Director of GCHQ.

28. On 23 December 2009 a submission was made seeking a direction in respect of two discrete sets of data in relation to the networks operated by a CSP. The limitation on the scope of data to be provided had been agreed between the CSP and GCHQ. That submission did specify the type of communications which the direction was intended to cover, and clearly set out the necessity for the making of a direction limited to those classes of data. The direction was made on 6 January 2010 but was in general form applying to all communications through the networks operated by the CSP, notwithstanding the agreement with the CSP as to the limited scope of the data to be required. The requirements made by GCHQ were not set out in a trigger letter but were communicated orally to the CSP.

29. On 20 October 2011 a submission was made seeking a direction replacing some directions which had been made earlier. The submission specified the data to be drawn from the networks operated by the CSP. However the submission sought a general direction, noting that the direction would potentially allow GCHQ to request data relating to all communications through the networks operated by the CSP, but that "*in practice requests have always been limited to sub-sets of data judged by GCHQ to be relevant to meeting [JIC] requirements for secret intelligence*". The direction made on 4 November 2011 was unlimited in scope, applying to all the networks operated by the CSP. The requirements made by GCHQ were not set out in a trigger letter.

30. On 4 July 2012 a submission was made seeking a direction. That submission did specify, with reasonable clarity, the type of communications which the direction was intended to cover and clearly set out the necessity for the making of the direction. The direction was made on 14 July 2012 which did adequately specify, in line with the submission, the type of communications which would be covered. The requirements made by GCHQ were not set out in a trigger letter. A further direction was made on 7 November 2012 in respect of another aspect of the networks operated by the same CSP. The submission and direction were in the same form as previously, identifying the particular category of communications data sought. The requirements made by GCHQ were not set out in a trigger letter.

31. On 10 September 2012 a submission was made seeking a general direction and set out in general terms the necessity for the making of the direction. The submission noted

the wide scope of the direction sought, but stated that in practice requests had always been limited to sub-sets of data judged relevant to intelligence requirements. The submission noted that the ISCom had recently taken on the role of overseeing the use by GCHQ of data it acquired under the authority of s 94. The direction made on 16 September 2012 was unlimited in scope applying to all the networks operated by the CSP. The requirements made by GCHQ were not set out in a trigger letter.

32. In June 2013 the Foreign Secretary had imposed a requirement to be supplied with six monthly reviews conducted by GCHQ into the use of s.94 directions. On 13 February 2014 the first such review was submitted. At that stage it was in short tabular form which did identify all the directions in force, and provided a general picture of the scope of data being obtained and its utility. By 2015 the reviews were more extensive. Those reviews listed the directions, identified the CSP to which the direction had been given, identified in shorthand the programme or type of data obtained, and gave a general description of the frequency of use and some illustrations of the use to which the data thus obtained had been put. Examples were given of the occasions on which the data had been used to identify subjects of interest, and the benefit that had been derived from such identification. In some cases the reviews resulted in data feeds being removed from the categories of data which were required under a direction. The reviews were in substance an internal audit of the communications data being obtained under the directions, an assessment of the value of the information thus derived and an assessment of the proportionality of continuing to require and use such data. The review also considered the necessity of continuing to treat as secret the making of s.94 directions. The reviews demonstrate the substantial operational benefit derived from data provided under the directions.

33. In his evidence the GCHQ witness stated that from 2012 any variation in data to be sought under a direction was required to be the subject of a submission to the Foreign Secretary. However from the closed documents it is evident that such a practice had commenced in 2010. The effect of these documents is that as at 4 November 2015, notwithstanding the wide scope of some of the directions in force, a procedure was well established under which the Foreign Secretary was, through the six monthly reviews, regularly informed of the scope of the communications data being received from each CSP, and had required any variations in the scope of data requested to be the subject of a submission and approval.

34. It has been noted above that from 2004 the IOCC had been made aware of s.94 directions obtained by GCHQ, and that he had subsequently reviewed the GCHQ compliance documentation which applied safeguards to the handling of, inter alia, data derived from the s.94 directions. After Sir Mark Waller was appointed as ISCom in 2011 he was made aware of the use of s.94 by GCHQ and was responsible for the oversight of use of data thus acquired. By 2014 the ISCom had inspected most of the s.94 directions which were being utilised by GCHQ.

35. In January 2015 the IOCC was asked by the Prime Minister to extend his oversight to include directions given under s.94. In October 2015 the Commissioner commenced a review of the acquisition of bulk communications data under s.94. In July 2016 the review was published. Amongst the findings of the review, at paragraph 8.42, was that the directions made by the Foreign Secretary:

- *"were very broad and provided a general description of communications data which was far wider than the requirement actually made of the (CSP), and*
- *the supporting documentation accompanying the section 94 direction then gave the specific details of the actual data sought including either by description and/or by the technical naming of the data; and*
- *the supporting documentation containing the specific data requirements has from time to time been modified to amend a data requirement …Each modification has been submitted to the Foreign Secretary for authorisation …"*

Amongst the recommendations was that s.94 directions for bulk communications data should indicate the specific communications data required to be disclosed.

36. In cross-examination of the GCHQ witness and in submissions, the Claimant pointed to the apparent discrepancy between the conclusions of the Commissioner set out above and the facts which emerged in the 10th witness statement of the GCHQ witness. Our findings set out above differ in some respects from those conclusions. It was not always the case that there were trigger letters to the CSP which specified the data actually required by GCHQ under the direction. Nor is it clear on the evidence that in all cases the direction made by the Foreign Secretary was either served on or made available to the CSP. Prior to 2010 there was no requirement that any variation in the data to be provided under a direction be approved by the Foreign Secretary [Review para 8.42]. The 10th statement of the GCHQ witness is not clear on this point, but his oral evidence that in some cases a requirement was communicated only orally would suggest that in those cases the direction was neither served on nor shown to the CSP.

37. As a consequence of the recommendation of the IOCC, it was decided that all extant s.94 directions should be replaced. On 14 October 2016 new directions were made by the Foreign Secretary which replaced all former directions made under s94 (1). The new directions were, as recommended by the Commissioner, more specific as to the categories of communications data required by the Director of GCHQ.

38. On 25 and 26 April 2017 IOCCO on behalf of the Commissioner carried out an inspection at GCHQ of the arrangements in place for the acquisition of bulk communications data under s.94 and its use. The inspection findings were summarised as follows:

> "*GCHQ emerged very well from this first inspection by IOCCO regarding the acquisition of bulk communications data. It was clear that the standards highlighted in review report of section 94 directions had been maintained. The inspectors were satisfied that GCHQ is acquiring bulk communications data lawfully within the permissible parameters of the Telecommunications Act 1984 and for the correct statutory purpose.*
>
> *A high standard of applications are produced for submission to the Foreign Secretary. GCHQ has taken full account of the recommendations in the IOCCO review report and integrated them into their processes*."

Further findings relevant to these issues were:

> (at page 4) "*The submissions to the Foreign Secretary were highly detailed, made explicit why the acquisition of BCD was required in the interests of national security, and the intelligence requirement or gap they were seeking to address. The submissions provided extensive detail as to how the BCD would*

address the operational requirement, the expected value of the intelligence to derive from the BCD, and why there was no appropriate or suitable alternative to the proposed conduct under the section 94 direction."

(at page 5) "*GCHQ undertakes reviews every 6 months as to whether the acquisition of BCD remains necessary and proportionate. The reviews are conducted in three parts:*

- *an audit of all current Directions;*
- *a quantitative assessment of the contribution to GCHQ operations of the data provided under these directions;*
- *a qualitative check on the value from data sources for which traceability to GCHQ outcomes is more difficult*."

39. It should be noted that those findings related only to directions issued on or after 14 October 2016. They are consistent with our findings in respect of those directions.

40. The 4th open witness statement of the GCHQ witness had not given an accurate picture of the process under which the directions prior to 14 October 2016 had been made and implemented. As the files of all s.94 directions made by the Foreign Secretary had apparently been collated and made available to the IOCC in 2015 it is surprising that those files were not carefully examined before the 4th witness statement was made. It is also difficult to see how any detailed review of a number of the submissions and directions made between 2001 and 2012 could have missed the point that there were several submissions which explicitly reserved to GCHQ the discretion as to what data would be sought from the CSP, and in only a small number of cases was there any evidence of trigger letters on the files.

Legal Issues

41. The text of s.94, as amended from 25 July 2003, is set out at paragraph 9 above. The directions made on 29 November 2001, some of which were still in force on 4 November 2015, preceded the coming into force of the amendments made by the Communications Act 2003. In those cases s.94 had not required the Foreign Secretary, when making the direction, to make a judgment as to whether it complied with the principle of proportionality.

42. The issue of delegation depends on the proper construction of s.94 and the factual analysis of the purpose and effect of the directions made by the Foreign Secretary. It is accepted by the Respondents that the Secretary of State had no power to delegate to the Director of GCHQ the power conferred by s.94(1). In **Wade & Forsyth on Administrative Law** 11th Ed at page 260, in discussing the maxim *delegatus non potest delegare*, the author states:

> "*The vital question in most cases is whether the statutory discretion remains in the hands of the proper authority, or whether some other person purports to exercise it.*"

The issue is thus whether there was in substance a transfer from the Foreign Secretary to GCHQ of the effective power to impose a requirement on the CSP. The fact that in form the standard direction required the provision of communications data "*if requested by GCHQ*" would not in itself constitute delegation, provided that GCHQ requested only those classes of communications data which the Secretary of State had himself decided should be provided. In effect that phrase has the meaning that data

should be supplied as and when requested, and is dealing only with the mechanics of provision of the data.

43. The revised argument put by the Respondents at the hearing on 12 and 13 March 2018 is that the Secretary of State had power to give a general direction to the CSP requiring it to provide information as requested by GCHQ. The core of the argument was set out at paragraph 6 and 8 of the skeleton argument dated 8 March 2018 as follows:

> "*The Secretary of State could, without unlawful delegation, direct the CSP to provide a category of data with subsets of that data being in effect called off from time to time by GCHQ. The fact that the mechanism for operating the data provision involved decision making by GCHQ does not entail unlawful delegation by the Secretary of State. The provision of the subset and this mechanism was authorised by the Foreign Secretary; and the production of the data in this way was the subject of the direction made by the Foreign Secretary to the CSP. The authorisation of the greater (all categories of data referred to in the direction) encompassed authorisation of the lesser (eg sub-sets of it from time to time called off by GCHQ). … The Secretary of State in issuing a direction in this form has evidently concluded that it is necessary in the interests of national security for the breadth of the categories of data referred to in it to be provided.*"

44. The principal difficulty with that argument is the factual point that in most cases the submissions made to the Foreign Secretary do not support the proposition that it could be necessary in the interests of national security, let alone proportionate, to require the

CSP to make available to GCHQ the entirety of the communications data generated by its networks. To the contrary, in most cases where a general direction was made it had been made clear in the submission that there was only an operational requirement for the provision of data in respect of certain classes of communication, albeit that the data to be required in the future might vary in line with intelligence requirements. Where, in some submissions, the reason for making a general direction was addressed, the only reason advanced was to provide flexibility for GCHQ to select whatever subsets of data it might consider necessary. There was no suggestion in such written submissions that it was indeed necessary in the interests of national security for all communications data held by the CSP to be made available to GCHQ. Those submissions expressly noted that it would be GCHQ, not the Foreign Secretary, which would determine the scope of the sub-sets of data required to be provided by the CSP.

45. It is necessary to note the parallel provisions of sub-sections 94 (1) and 94 (2). The argument of the Respondents would lead to the conclusion that the "*directions of a general character*" made by the Foreign Secretary empowered GCHQ to impose a requirement on the CSP to do "*a particular thing*", i.e. to provide the communications data as specified by GCHQ, not as specified by the Foreign Secretary. The Respondents' argument now recognises that, in most cases, GCHQ officials made the decision as to which subsets of data were to be provided. It is no answer to the delegation argument to state that the Foreign Secretary had, through a general direction, authorised GCHQ to decide which data should be required to be provided by the CSP. Both general and particular requirements are, under s.94, to be imposed only by personal direction of the Foreign Secretary.

46. In answering the question whether the substance of the power to make a direction has been delegated to GCHQ it is necessary to take account of the way in which the general directions made by the Foreign Secretary were used in practice. Officials decided, in discussion with the CSP, what types of data the CSP could provide to meet a current intelligence requirement. The CSP would then be informed that the Foreign Secretary had made a general direction, but the effect of that direction would depend entirely on the datasets which GCHQ selected for provision. Where there was a letter to the CSP it was generally stated that the requirement would expire after 6 months, unless renewed by GCHQ, and that was in line with the submissions which had been made to the Foreign Secretary. The power exercised by GCHQ was thus a substantive power to determine the content and duration of the requirement to be imposed under the direction.

47. For those reasons we conclude that in cases in which the submission had sought a direction in order to enable GCHQ to obtain data relating to particular classes of communication (whether or not the submission specified those classes), but the Foreign Secretary made a general direction which applied to all communications through the networks operated by the CSP ("targeted requirement/general direction cases"), there had been an unlawful delegation of the power conferred by s.94(1). However, as noted above (at paragraphs 32 and 33), the Foreign Secretary had from 2010 imposed a requirement that any variation in the scope of data to be provided under a direction required his approval, and from 2014 the Foreign Secretary was supplied with regular 6 monthly reviews setting out in detail the scope and justification for the data being provided under s.94 directions. So by 4 November 2015 there was in substance no delegation of power from the Foreign Secretary to

GCHQ. The effect of the requirements imposed from 2014 onwards was that it was the Foreign Secretary, not GCHQ, who decided the scope of the continuing requirements to be imposed on a CSP under s.94(1).

48. The directions made on 14 October 2016 did, as recommended in the review conducted by the IOCC, specify the scope of the data requirement imposed on the CSP. The Claimant submits that there was delegation in these cases, but only on the ground that the form of the directions continued to include the words "*if requested to do so by GCHQ*". That is a point of formalism, not substance, because the closed documents make clear that the scope and effect of the directions were determined by the Foreign Secretary. The letters of request, accompanied by the direction, sent by GCHQ to each CSP (a redacted example of which is at GCHQ 13) were fully in line with the submission on the basis of which the Foreign Secretary had made the direction. Those directions, as confirmed by IOCCO in its review, properly specified the datasets which the CSPs are required to provide. Under those directions there was no impermissible delegation to GCHQ officials.

49. Under s.94 (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*."

In the case of general directions made after subsection 2A came in to force on 25 July 2003, the Foreign Secretary was thus required to consider whether the conduct required by the direction, that is the provision to GCHQ of all or any of the communications data held by the CSP, was proportionate to the necessity to meet an

intelligence requirement in the interests of national security. In those targeted requirement/general direction cases in which the submission sought only a direction under which GCHQ could obtain particular classes of communications which were of current intelligence interest but the direction made was of general scope, applying to all communications through the specified networks operated by the CSP, the direction went further than was required to achieve the legitimate and necessary aim of securing access to the communications data which GCHQ actually required. In those cases where such a general direction was made after 25 July 2003, it did not comply with the requirements of subsection 2A.

50. The Claimant puts its argument primarily on the impermissibility of delegation to GCHQ, an argument which Mr. De La Mare QC at one stage described as a technical point. But the wide scope of the directions made by the Foreign Secretary raises a more substantial point as to whether such directions, which fail to define the categories of communications to which they apply, could, even if lawfully made under s.94, be treated as "in accordance with the law" under Article 8. In the Claimants' reply argument dated 13 October 2017 at paragraphs 10 & 11 the point was made that it would not be permissible for GCHQ to exercise the scope of discretion purportedly conferred under the standard form general directions, so those directions were not in accordance with the law.

51. In the First Judgment at paragraph 62 we stated that in considering whether measures are compatible with Article 8 as being in accordance with the law:

"*There must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action. We must be satisfied that there exist adequate and effective guarantees against abuse*."

In those targeted requirement/general direction cases referred to at paragraph 47 above the general form of direction did not comply with that test. The scope of any requirements which could be made by GCHQ under the directions was limited only by reference to the networks identified in the direction, not by any limitation on the categories of communications in respect of which data could be obtained. The scope of the data to be obtained is not specified in the direction, but in practice was communicated to the CSP only through a trigger letter or an oral requirement from GCHQ. In theory the agency could have used the general form of such directions to impose on the CSP a requirement to produce communications data which extended beyond the scope of any data requirement which had been sanctioned by Foreign Secretary, a point which was expressly acknowledged in some of the submissions made. Sub-sections 3 (2) and 4 (2) (a) of the ISA would have prevented GCHQ from requiring the provision of data otherwise than in the interests of national security (or for other statutory purposes) but provided the data was required for such purposes the general directions gave GCHQ unfettered discretion as to the requirements to be imposed upon a CSP. In form a general direction was a *carte blanche*. In practice it was not treated as such, and there is no evidence that GCHQ ever sought to obtain communications data which fell outside the scope of data which had been sought in the submission to the Foreign Secretary. After about 2010 any variation in the scope of data sought under a general direction was the subject of a submission to and approval by the Foreign Secretary. Since the practice of requiring 6 monthly reviews was instituted in 2013 and full oversight by the IOCC commenced in 2015, any

arbitrary use of the directions would have been most unlikely to have escaped scrutiny. In general it appears that from at least 2014 onwards great care was taken to ensure that the Foreign Secretary was made aware of and approved the scope of the requirements being imposed on CSPs.

52. But the existence of those controls is not an answer to the point of principle that the form of general directions employed, if otherwise valid under the provisions of s.94, did purport to give unfettered discretion to the agency as to the type of communications which should be treated as covered by the direction. The lack of legal control on the discretion of the agency is compounded in those cases where the specific requirement was not communicated in writing to the CSP. The CSP would not be in any position to question the scope of the requirement communicated, because the CSP would have no knowledge of the limited basis upon which the direction had been made, and on the face of the general direction (if provided) the CSP was required to produce any data which GCHQ requested. In those targeted requirement/general direction cases referred to at paragraph 47 above, the form of the general direction made by the Foreign Secretary did not comply with the requirement under Article 8 that measures taken by the state should be in accordance with the law.

53. For those reasons we conclude that most of the relevant directions made between 29 November 2001 and 7 November 2012 were not lawfully made under s.94. In the closed judgment we list the relevant directions which remained in force on 4 November 2015 and set out in summary form our reasons for determining whether or not each of those directions complied with the legal principles set out above. Applying Rule 6 of the Investigatory Powers Tribunal Rules we conclude that it

would be contrary to the interests of national security to identify either the identities of the CSPs in respect of which directions were made, or the number of such directions in force at any particular time. In each case disclosure of such information might risk giving indications as to the coverage of directions issued. In accordance with the guidance given by the Court of Appeal in **R v Secretary of State for Foreign and Commonwealth Affairs ex p Sarkandi** [2015] EWCA Civ 867 at paragraph 26, as much information as can properly be disclosed is set out in this open judgment.

54. It is important to note that, although some of the directions were in our judgment not lawfully made under s.94, on our review of the closed documents we are clear that the actions taken by GCHQ to obtain BCD under the general directions made by the Foreign Secretary were limited to the classes of communications data which had been sought in the submissions, and were clearly necessary in the interests of national security, and proportionate. The 6 monthly review reports prepared by GCHQ from 2014 onwards carefully reviewed the scope, operational need and proportionality of the actual requirements imposed in order to acquire BCD. On the closed evidence, the operational intelligence need for the data requested, and the proportionality of using s.94 as the only practical means of obtaining such data, is very clearly established. The broad scope of the general directions did not in practice lead to the provision of any BCD which could not lawfully have been required under s.94, within the limits prescribed by Article 8.

55. It was entirely understandable that in the aftermath of the 9/11 attack on New York the directions made in November 2001 should have been drafted broadly so as to

allow GCHQ to vary the data it sought as intelligence requirements rapidly developed. But the scope of those directions should have been reviewed after s.94 was amended in 2003. By 4 November 2015 adequate and effective arrangements were in place (as set out at paragraph 33 above) to ensure that the acquisition of BCD by GCHQ was regularly monitored and reported, and any variations in the extent of data collected required to be approved by the Foreign Secretary. So in practice by 2014 it was the Foreign Secretary who determined the scope of data collection permitted under all directions which remained in force. In addition, from October 2015 the acquisition of BCD under s.94 directions was subject to oversight by the IOCC. The fact that after extensive disclosure of documents, to the parties in open evidence and to the Tribunal only in closed evidence, and detailed submissions, we have concluded that some of the directions were not, when made, lawful, does not indicate that oversight by IOCC after 4 November 2015 was ineffective. To the contrary, the core recommendation made by the Commissioner in his careful review published in July 2016 was that the directions made by the Foreign Secretary should not be in general form but should specify the communications data to which they were intended to apply. That is substantially the same point that underlies our own decision on the legality of some of the s.94 directions made by the Foreign Secretary.

56. The Claimant argues at paragraphs 61 and 62 of its skeleton argument dated 22 September 2017, that in the light of the change in the evidence from GCHQ the submissions made by the Respondents to the Tribunal at the hearing held in July 2016 were materially misleading. We are not persuaded that those general statements that the s.94 directions had been made by the Secretary of State were misleading. However it does follow from the conclusions reached above that the submissions

made in the Respondents' Skeleton argument dated 6 October 2017 at paragraphs 62 to 68, in asserting that the selection of data had been the decision of the Secretary of State, cannot be supported. Those submissions were based on the 4th witness statement of the GCHQ witness which was materially inaccurate.

57. On the basis of the evidence reviewed above we are satisfied that the acquisition of bulk communications data under lawful directions made under s.94 by the Foreign Secretary on 14 October 2016 was and remains necessary and proportionate.

Issue 2: Consequences

58. We have considered the precise terms of the declaration which we made following the First Judgment, namely that "*the Respondents' regime under section 94 of the Telecommunications Act 1984 was not in accordance with the law under Article 8(2) ECHR until 4 November 2015, but has been in accordance with the law under Article 8(2) ECHR since that date*" (emphasis added). In the light of this Judgment the words underlined cannot stand. The October Judgment falls to be reopened by virtue of our consideration of the directions, and the reconsideration of the matters the subject of Issue 1, and we have concluded that many of the directions, which continued after 4 November 2015 until 14 October 2016, were unlawful. Our attention has been helpfully drawn by the parties to the useful discussion and reference to authorities in **Wade &Forsyth** pp 247-254, and **Craig Administrative Law (7th Ed)** at 24-011 p749, and our task, as we see it, is to consider, in the light of that guidance, what remedy to grant in the light of our conclusions, and to exercise our discretion accordingly.

59. Notwithstanding the submissions of the Claimant, we do not propose to quash any directions or to make any declaration as to their effect, for the following reasons:

(i) The effect of our conclusions on Issue 1 is that a number of directions made by the Foreign Secretary were not lawfully made, but that in substance and effect from about 2014 there was no unlawful delegation of power, nor was there a disproportionate use of such directions. For the reasons set out at paragraphs 54 and 57 above, the evidence is that the communications data obtained by GCHQ under such directions was within the proper scope of s.94(1) and the acquisition was both necessary and proportionate.

(ii) We bear in mind the potential effect on third parties, the CSPs, who had no reason to believe that the directions, compliance with which was being required, were other than lawful.

(iii) For the reasons set out in paragraph 53 we are not able to identify in open which directions were lawful and which unlawful, and hence, even if otherwise minded to do so, we would not be in a positon to quash some and not others.

60. Consequently no declaration will be made, nor any further relief granted, in respect of communications data obtained by GCHQ under those directions which were unlawfully made whether prior or subsequent to November 2015.

Issue 3A: Sharing with Foreign Agencies.

61. The issue for us so far as the ECHR is concerned is, as we said in paragraph 59 of our First Judgment, to which we refer, framed by reference to the "in accordance with law" requirement in Article 8. We referred in paragraph 3(iii) above to the need for

assumptions because sharing of BCD and BPD with foreign agencies is not admitted by the Respondents. The application of the NCND ('neither confirm nor deny') principle to this question is well explained by the SIS witness in his witness statement of 1 February 2017, pertaining as it does to operations, capabilities and relationships which cannot be disclosed into the public domain without damage to national security, and we accept it. The fact that unauthorised and unadmitted disclosures have been made by a former US contractor, Mr Snowden, though it may lead on to or prompt inquiry or investigation, cannot possibly amount, or be equivalent, to admission or avowal by the Respondents. There is a sixty year old public international agreement, relating to the sharing of intelligence, between the countries which are called the "Five Eyes", namely, the UK, the United States, Australia, New Zealand and Canada. There is no reference in that agreement to BCD or BPD, nor to the safeguards which would be applied if there were sharing of BCD or BPD. The absence of sufficient evidence to enable the Tribunal to be satisfied as to compliance with Article 8, in the event that there were such sharing of BCD or BPD, led us, in paragraph 95 of the First Judgment, to leave this issue outstanding. There were detailed procedures in place. The Handling Arrangements in respect of each of the Agencies with regard to both BCD and BPD, which were published in November 2015, on the face of it were applicable to any sharing which might occur with foreign Agencies, and they were set out in Appendix A to the First Judgment. Strict rules relating to the disclosure of BCD outside the Agencies were set out in paragraphs 40 to 43 of the section relating to BCD and in paragraph 47 of the section relating to BPD. We did not however have the full opportunity to consider the position in detail.

62. There has subsequently been more detailed disclosure as to the safeguards applicable in the event of any sharing taking place, which were set out in a detailed appendix to

the Respondents' skeleton for the October hearing, and which we append to this Judgment as Appendix 2. In paragraph 9 of the second amended witness statement of the GCHQ witness, he clearly set out the following; -

> *"Whilst we can neither confirm nor deny whether the SIA have agreed to share or in fact do share BPD/BCD with either foreign liaison partners or LEA, were we to do so we would*
>
> - *Follow the principles and approach set out in our respective handling arrangements and policy/guidance*
>
> - *Take into account the nature of the BPD/BCD that was due to be disclosed*
>
> - *Take into account the nature/remit of the body to which we were considering disclosing the BPD/BCD*
>
> - *Take into account the approach taken by any other SIAs who may have shared bulk data and have regard to any protocols/understandings that the other agencies may have used/followed.*
>
> - *Depending on the individual circumstances seek assurances that the BPD/BCD in question would be handled in accordance with RIPA safeguards i.e. that it would be disclosed, copied, distributed and retained only to the minimum extent necessary for the purpose of RIPA (in the interest of National Security, for the purpose of preventing or detecting Serious Crime or for the purpose of safeguarding the economic well-being of the UK).*

- *If relevant to the particular circumstances, seek assurances that its use was in accordance with the UK's international obligations.*

- *Any data shared with the organisation would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance or approved through the Action-on process. Action-on is a process which is used by each of the Agencies."*

63. As is our normal practice, we have held open hearings on the hypothesis that the fact that such sharing has taken place is to be assumed. In any event, the Tribunal has been able to see, by virtue of disclosure made by the Respondents, and the holding of the closed hearing, whether there has been such sharing and, if so, whether the Handling Arrangements have been applied.

64. Lawful operation, so far as concerns Article 8 of the ECHR of the sharing arrangements for BCD/BPD with foreign Agencies, depends, in the light of our previous Judgments, in which we have considered and set out the law in this regard, upon:-

(i) the existence of adequate safeguards against abuse by the Executive.

(ii) sufficient disclosure of the capability to share, and of such safeguards, for the purposes of the test of foreseeability. We are satisfied that the disclosure of the Handling Arrangements in November 2015 was a sufficient disclosure for the purposes of the test of foreseeability, which does not require, in the field of national security, the disclosure of any greater detail.

(iii) the existence of sufficient oversight arrangements.

65. We have, as set out above, considered both open and closed evidence. On the assumption that sharing of BCD and BPD with foreign Agencies by any of GCHQ, MI5 and SIS might occur, what is necessary is that consideration be given by them to such proposed sharing:-

(i) as to whether it is necessary and proportionate to supply BCD and/or BPD in whole or in part to such Agency.

(ii) as to whether in relation to such sharing, the relevant Agency can be satisfied that, as far as possible, the arrangements which ensure the security of BCD and/or BPD in their custody can be replicated in the hands of the recipient. This would be achieved in relation to those recipients who have been regularly trusted in the past. In any given case, and certainly in relation to those recipients where such are not, or are no longer, in that category, then due diligence, or what SIS called an "*information gathering exercise*", would be carried out at the time.

(iii) by ensuring so far as possible that there is control over what is supplied and therefore that sanctions can be applied in the event of non-compliance, and we considered the existence, operation and effectiveness of what is called the "*Action-on policy*", referred to in paragraphs 31 and 71 of Appendix 2.

66. There was discussion at the open hearing as to whether there was a difference between the approach of GCHQ and that of the other two Agencies in relation to the degree to which the protection to be given to the data would be 'substantially equivalent' in the hands of the recipient, but we are satisfied that, whatever the wording used in the underlying rules, only the degree of urgency in a given case might reduce the consideration of such substantial equivalence, and even then only in

relation to a trusted recipient, and that there are sufficient safeguards in the system in place with all three Agencies. No data could be shared without full prior consideration of the nature, remit and security arrangements of the proposed recipient, and without prior authorisation of a senior officer.

67. We turn to the question of oversight, on the hypothesis that such sharing might have occurred. In the context of oversight, we need to address what is required in order to amount to adequate oversight, so far as we can form a view on the evidence before us.

68. Our attention has been drawn to the following guidance:-

(i) in **MK v. France** Application 19522/09 ECtHR 18 July 2013 at paragraph 41, the Court appears to have taken the view that the test in considering the viability of a safeguard – or, in our case, of supervision - was whether it was "*practical and effective"* rather than "*theoretical and illusory"*.

(ii) In **R (Catt) v. ACPO** [2015] AC 690 at para.33, there was discussion about a system of safeguards within the context of the ECHR, which suggested that a system could be satisfactory even though it was not proof against mistakes, from which the parties before us drew a conclusion that what was critical was that there was no 'systemic' failure.

(iii) In **Zakharov v. Russia** [2016] 63 EHRR 17 at para.302, the Grand Chamber, addressing the need for adequate and effective guarantees against arbitrariness considered compliance with "*the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice.*"

69. We would suggest the following approach:-

(i) The fact that errors occur in the handling of data does not necessarily establish that safeguards or oversight were not effective; no oversight can be expected to prevent any errors occurring.

(ii) The mere fact that errors are reported, or are detected by internal or external audit, may be evidence that the oversight system is working, not that it is defective.

(iii) There is a duty on the Agencies (now statutory in the IPA 2016 at s.235) to report to the Commissioner anything that is material for the Commissioner to know in order to perform his oversight function properly; if there has been a failure to report a material use of data, of which the Commissioner might not be aware, such as disclosure of data to Industry Partners, then that is to be treated as a failure - in that respect - to ensure proper safeguards and oversight.

(iv) A Commissioner has a considerable margin of appreciation as to what resources he needs to perform his functions correctly, and there are no grounds for criticism of his decisions as to how he applies those resources; it is not the function of the Tribunal to audit the performance of a Commissioner's functions; the fact that a new Commissioner might take a different view on an issue does not establish that there were not adequate and effective arrangements before.

(v) The question may well be capable of being resolved by reference to whether there has been a systemic failure in oversight arrangements, not whether in particular respects the performance of the Agencies can be criticised.

70. We have considered the information supplied by IPCO. We are satisfied, by virtue of the previous divided responsibilities of the Commissioners, to which we referred in paragraph 6(3) above, that IPCO did not have available all the previous records or information which we have been able to see in CLOSED. We note in particular the letter dated 28 November 2017 from the present Commissioner, Sir Adrian Fulford who, after quoting numerous extracts from earlier Reports, concludes that it would be incorrect to infer from what had been said in the IPCO correspondence that '*the approach adopted by the predecessor organisations were either less than rigorous or effective"*. In any event, we refer to evidence of oversight in our accompanying CLOSED Judgment.

71. The majority is satisfied that, in the circumstances which we have considered in open and in closed, the regime in respect of sharing BCD and BPD was compliant with Article 8. There are two dissenting Members, Mr. Flint QC and Ms O'Brien QC, each of whom has set out reasons for dissent in respect of Issue 3A in our CLOSED Judgment.

72. As for the position under EU law, in relation to transfer of intelligence out of the EU to foreign agencies, that must obviously await the outcome of the Reference to the CJEU.

Issue 3B:- Sharing with LEAs.

73. There is no admission by the Respondents that any BCDs or BPDs are provided to, or shared with, LEAs. There is however no challenge to the supply to LEAs of the product of information derived lawfully by the Agencies. If there were such sharing of BCDs, or BPDs, then there would be the same safeguards as appear in the Appendix to this Judgment. The Claimant submits that supply by the Agencies to the LEAs of

BCDs and BPDs, if that occurred, would be a breach of the **Padfield** principle [1968] AC 997, because there would be an evasion of the restrictions on acquisition of information by the LEAs imposed by the provisions of RIPA. However, the Respondents submit that it would be lawful for GCHQ to provide data obtained by means of s.94 directions to LEAs, on the basis that those other LEAs required the data for the purposes of combatting serious crime. GCHQ obtains data pursuant to s.94 in the interests of national security, which is one of its statutory purposes as listed at s.3(2) of ISA. The Respondents then rely upon s.19 of the Counterterrorism Act 2008 ("CTA"):-

"(2) 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.

…..

.*(5) Information obtained by GCHQ for the purpose of any functions may be disclosed by it -*

(a) for the purpose of the proper discharge of its functions or

(b) for the purpose of any criminal proceedings."

74. Given that GCHQ may exercise its statutory functions in support of the prevention or detection of serious crime under s.3(2)(c) of ISA, GCHQ is entitled to use s.94 data for that other statutory purpose, as well as in the interests of national security, and so is entitled to disclose s.94 data to LEAs for that purpose. Any such disclosure must comply with the necessity and proportionality requirements imposed by s.6(1) of the

Human Rights Act, and s.4(2) of ISA provides that it is the duty of the Director of GCHQ 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."*

75. An LEA may only exercise a power to acquire communications data by RIPA Chapter 2, but the issue here concerns the power of an agency to share, without the need for the LEA to exercise any statutory power. The power under s.19 of the CTA is very clear, and there is no basis for implying in such power to disclose a restriction to the effect that such data may not be disclosed to an LEA. S.19(5) of course postdates RIPA, and we are satisfied takes it into account, and is not to be read down in the light of it. The Agency, having lawfully acquired the data under s.94 in the interests of national security, is permitted to make onward disclosure within the terms of s.19(5). This does not circumvent any restriction in s.94 relating to the acquisition of data. Additionally, quite apart from the fact that RIPA remains the ordinary route for the LEAs to obtain data, in any event there is no evasion of any substantive protections in s.22 of Chapter 2 of RIPA. The basic principles of necessity and proportionality apply both under s.22 and to the power of the Agency to disclose under s.19 of the CTA (having regard to s.4(2) of ISA and the Human Rights Act). The information could not be arbitrarily disclosed under s.19. There is thus specific statutory authorisation for GCHQ to use s.94 data for the purpose of prevention or detection of serious crime and its disclosure for that purpose.

76. We are satisfied in the circumstances which we have considered in open and in closed that if there were sharing of BCD or BPD with LEAs, such activity would fall within the oversight given by the Commissioners since 2015, and that there has been since November 2015 sufficient disclosure of the safeguards under which it would take place to satisfy the requirements of foreseeability.

77. That resolves the issues relating to domestic law and the impact of the ECHR. It may be, however, that if there is sharing of BCD obtained under a s.94 Direction with LEAs for the purposes of the investigation of serious crime, the issue so far as EU law is concerned would need to be reconsidered after the outcome of this Tribunal's Reference to the CJEU. The Respondents have set out in paragraph 61.2 of their Skeleton Argument dated 6 October 2017 why they contend that any such sharing would fall outside the scope of the EU Treaty and of the e-Privacy Directive. Referring *inter alia* to paragraph 48 of our Second Judgment, they state that such sharing would not amount to an activity of any provider of electronic communications services, and so (even if falling within the EU Treaty) would be excluded from the scope of the e-Privacy Directive, and that the CJEU's decision in **Opinion 1/15 (ECL1:EU:C2017:59)** should not lead to a different decision. That may remain for consideration after the outcome of the Reference.

Issue 3C: Sharing with Industry Partners

78. It is common ground that it is important that there be stringent protection of such data. This Issue began as one area for consideration, and in the course of the hearings it included a wider issue, to which the title of this Issue is somewhat inapt. As originally addressed, sharing with industry partners took in the supply of data, or the grant of remote access, to those specialist contractors who could assist with design,

testing, operation and maintenance of systems. GCHQ has avowed this. Insofar as it involved the University of Bristol, this was not regarded as supply or sharing outside of GCHQ, because there is a fully integrated research department there, in GCHQ's premises in Bristol, under the control of GCHQ staff stationed there, although there has in the event been no sharing of BCD or BPD with Bristol. However, there is use made of specialist contractors, all of whom are fully vetted, and, although, wherever possible, data shared with industry partners will be held on GCHQ premises, where most systems development takes place, failing that, the data must be held on secure and accredited corporate premises in the UK, and there has been on only one occasion limited remote access by industry partners to BPD or BCD. There was some limited sharing of data with such contractors, which may have contained BCD, in 2010-11, but not of BPD since 2010. The data is only transferred under cover of a Raw Data Release Request Form, but in each case only for the purpose of research or development, to GCHQ accredited premises and to contractors who are subject to the same training, vetting and compliance monitoring as GCHQ employees. The safeguards are set out in full in paragraph 41 of Appendix 2 to this Judgment, to which we refer, and, we have been told, are stringently operated.

79. Although the involvement of industry partners in GCHQ's activities was disclosed in general terms to the Commissioners, the issue of supply of data to such contractors was not the subject of oversight by them, until disclosed in these proceedings in 2017. This was plainly a failure of oversight, in the sense that this important but relatively small area of activity was not looked at by the Commissioners, although it was in fact the subject of safeguards imposed and operated by GCHQ itself. We shall return to this when we consider the case made by the Claimant in respect of oversight by the Commissioners.

80. The other area which has, as discussed above, fallen into this Issue is not strictly a question of sharing with industry partners, but the use of contractors within the Agencies, primarily GCHQ. This was known to the Commissioners, who, in their Confidential Memoranda, in addressing and reporting on the occasional failures which occurred, would note whether such failures were by a permanent employee or a contractor.

81. Those contractors working within the agencies are heavily vetted, in the same way as full-time employees, and of course are subject to the same disciplinary and statutory obligations as permanent employees. On the evidence there has been no greater risk from the use of properly vetted contractors than from that of employees. Nevertheless, we were disappointed that inaccurate information was given to the Tribunal, and thus to the Claimant, as to the number of such contractors with Privileged User accounts, a failure the significance of which Dr. Gus Hosein, an Executive Director of the Claimant, highlighted by pointing out the importance of the role that a Privileged User with administrative rights could play. However, GCHQ has systems to guard against any misuse. This was one of those cases, to which we referred in paragraph 6(iv) above, where the inaccuracy of the evidence caused us concern, but it does not lead us to conclude that the system has failed, or that there is an absence of the safeguards required by Article 8.

82. Sir Mark Waller has confirmed that he was unaware of any industry sharing of BPD. There is no good reason why he was not briefed about the remote access arrangements to BPD so that he could consider whether they were justified and robust. This is a failure of oversight, not caused by Sir Mark, but by GCHQ. The process of oversight requires co-operation between the overseer and the overseen, and it is the judgment of

the Tribunal that setting up an arrangement which enables an external contractor to access remotely data held by GCHQ is a step of sufficient importance to require justification on each occasion when it happens. It is also important enough to require oversight, if the Commissioner thinks it necessary. That means that it must be communicated to the Commissioner. The very limited extent of the arrangement may have meant that the Commissioner would not have scrutinised it further, but he ought to have been able to decide that for himself.

83. It is clear from the confidential annexes to Sir Mark Waller's Reports for 2015 and 2016 that he carried out oversight of BPD across the three agencies.

a. In 2015 he scrutinised in detail BPDs across the three agencies. This represented a reasonable sample. He approves of the way in which MI5 and SIS deal with this material. In respect of BPD at GCHQ he explains the controlled way in which only a minority of GCHQ staff have access to BPD. He does not say that he is aware that anyone other than GCHQ staff has any access at all. He identified inadequacies in paperwork at GCHQ which caused him to express "deep concern" in one respect. He was also informed during an inspection that a BPD had been shared with the other agencies without prior authorisation in breach of the handling arrangements. He concluded

> "*I welcomed that GCHQ raised this error and acknowledged the urgent nature of the situation, however the Handling Arrangements are clear and must be followed even in urgent situations.*"

b. Sir Mark was certainly aware of the use of contractors by the UKIC. In the 2015 Confidential Annex, Sir Mark identified breaches by a contractor in relation to MI5 protective monitoring measures, not related to BPD. There

was also one such breach by a contractor in relation to BPD which he took *"very seriously and wanted to know what action would [*be taken*] in relation to [*the*] employee."* He also reviewed the protective monitoring of the BPDs held by SIS and GCHQ. In relation to GCHQ he noted that in the first half of the year some investigations were triggered by the system. They revealed that all the searches concerned had a legitimate business reason and were both necessary and proportionate. The 2016 Confidential Annex also revealed a serious breach at MI5 by a user and a relative minor breach by a contractor. He recommended that MI5 should make it clear to all seconded staff and contactors working there that they are subject to MI5 rules of conduct. He was informed that a member of staff at GCHQ had tried to leave the building with a Top Secret document. He was arrested and "other material" was found when his home was searched. No charges were brought.

c. Sir Mark was aware specifically that GCHQ used external contractors on its sites. This was not connected with BPD, but means that it would not be true to say that he did not appreciate that this practice occurred. His suggestion that he did not know about industry sharing is to be read with this in mind. He did not know that industry partners had direct access offsite to BPD.

d. The potential risk arising from permitting external contractors to have privileged user rights as explained by Dr. Hosein is not mentioned in any of Sir Mark's reports and it is not known whether he was aware of this.

84. The Tribunal considers that some bulk datasets have a commercial and, perhaps, political potential value. This means that access to them by those who may have the interests of their employer (a commercial concern) at heart, when there may be a

conflict between those interests and the national interest in the proper functioning of GCHQ, should be the subject of the most careful safeguards and oversight. It is clear from the evidence of the GCHQ witness that the general rule is that data is not transferred to such external bodies, nor do they have remote access to it. However, the exceptions identified above, isolated as they appear to be on the evidence, demonstrate in our judgment an inadequate appreciation of the risks involved to the privacy rights of those whose data has been harvested and stored. We do not consider that this represents a systemic failure such as to render either that harvesting or storage, or the oversight of it, unlawful. We do consider that it is for GCHQ to escalate the significance of this activity to an appropriate level of priority, and for IPCO to consider how it should be overseen in future.

85. As far as the use of external contractors at UKIC premises is concerned, the Tribunal accepts that this is not "sharing" in the sense used in setting the parameters of this claim. Whether it is right that it poses no extra risk as against using directly employed staff is a matter which needs to be kept under review in the light of experience. No doubt the management of the risk depends on the vetting, protective monitoring measures, active supervision and on the oversight of the effectiveness of those factors. It also depends upon measures being in place to ensure that staff and contractors all operate in ways which infringe privacy rights to the smallest extent possible. Thus contractors, and directly employed staff, should only have access to the operational data which they need in order to fulfil the task in hand. We are told by the GCHQ witness that this is the method of operation at GCHQ. We do not consider that the approach to the use of contractors on site as explained by him renders the use and acquisition of BCD/BPD unlawful.

86. In the circumstances which we have considered in open and in closed, we resolve Issue 3C in favour of the Respondents.

Issue 4: Proportionality

87. The issue of proportionality is, of course, entirely different from, and supplementary to, the question of necessity. As the Claimant has emphasised and accepted, there is no doubt that the use of BCD and BPD is of great value in the protection of national security, and the Anderson report has so confirmed and reiterated, with considerable examples of crucial value, to which we have also referred in our earlier Judgments. But although that will obviously weigh in the balance, it does not wholly resolve the separate issue of proportionality. Both parties accept that the legal position is well addressed by Lords Reed and Toulson, giving the Judgment of the Supreme Court in **R (Lumsdon) v The Legal Services Board** [2016] AC 697 at para.105, namely that the question is *"whether a less intrusive measure could have been used without unacceptably compromising the objective"*, in this case of protecting national security. It is not simply whether a less intrusive measure could be adopted, but whether the legitimate aim of protecting national security could be equally achieved by less intrusive measures.

88. It is in this context that we have been asked to consider whether we would be assisted by the appointment of an expert, or team of experts, to advise us: indeed the Claimant effectively submits that we cannot be satisfied as to the proportionality of the measures taken by Agencies, which have been subject to oversight by the Commissioners, without instructing such an expert. The question would be what the expert's task or remit would be; presumably it would be to examine the measures taken by the Agencies by way of acquiring and accessing and using the data, in order

to consider whether the same objective could have been reached by taking a less intrusive course, by way of an alternative measure, which either is or might become available. We recognise that this course is now open to the Commissioner, although it is not clear to us as to whether he has yet taken advantage of their advice, as a result of s.246(1) of the IPA 2016, whereby the Commissioner is obliged to:-

> "*ensure that there is a Technology Advisory Panel to provide* [him], *the Secretary of State and the Scottish Ministers about -*
>
> > *(a) the impact of changing technology on the exercise of investigatory powers whose exercise is subject to review by* [him],
> >
> > *(b) the availability and development of techniques to use such powers while minimising interference with privacy."*

89. If and when the Commissioner makes use of that opportunity, it will clearly be of assistance in facilitating an important part of his job, namely to suggest and encourage change and improvements. We note that the statute did not specifically make provision for this panel to be available to the Tribunal, although plainly we could ask the Commissioner for such assistance if required. Our task is, however, very different from the Commissioner's. It is to see whether we are satisfied that what has occurred in the past, while supervised by the Commissioner, and always subject to the suggestions of improvements, which, as we have had the opportunity of seeing for ourselves, have regularly been made, has been proportionate or, as Mr Jaffey QC put it in the course of his submissions "*appropriately calibrated to the circumstances"*. An important part of such consideration by us is to see whether, when the Commissioner or his team makes recommendations, such recommendations are suitably and timeously complied with. We conclude that it is not necessary for the

purposes of our present task to introduce yet another layer of investigation by way of instructing experts.

90. The Claimant raises questions by reference to machine learning, to artificial intelligence, to the use of social media intercept, and whether any of such techniques have been adopted by any of the Agencies, and if so whether any more or less proportionate or intrusive methods could have been used. But this assumes that such techniques have been adopted, and the Commissioner and his team have the fullest opportunity to examine them.

91. The analysis that we have carried out in paragraphs 8 – 58 above in relation to s.94 shows that, whereas GCHQ has been fully mindful of its obligations as to bearing in mind both necessity and proportionality in obtaining data pursuant to s.94 directions, the directions themselves are in many cases not so limited. That is a factor which indicates that at the stage of acquisition of BCD, GCHQ had its obligations well in mind.

92. It is significant that there is no criticism by the Claimant of the safeguards set out in Appendix 2 to this Judgment, especially at paragraphs 29, 80 and 81, relating to the regular consideration of proportionality by the Agencies at each stage of acquisition of and access to BCD and BPD and the reduction of intrusiveness by the filtering out of irrelevant material. We have set out in our CLOSED Judgment our conclusions about the way in which the system has operated in practice. It is quite clear that the Commissioners were extremely diligent in chasing up and questioning compliance by the Agencies with regard to proportionality. The examples which the Claimant has rightly drawn to our attention, of the making of 'amber warnings' in relation to the need for improvement, and the comments by Inspectors that an Agency has "*fallen*

short in providing complete assurance" in relation to consideration of proportionality, seem to us to be part and parcel of the interplay between the oversight and the overseen, leading on occasion to recommendations which would *"enhance the oversight"* given by the Commissioner. Criticisms are on occasion mixed with compliments.

93. We have noted above that in relation to the recent correspondence from IPCO there does not seem to have been a thorough analysis of the records that had previously been kept by the two separate Commissioners, a difficult problem in itself as we have commented in paragraph 6 (iii) above, at least until the personal involvement of Sir Adrian Fulford in his clarification letter of 28 November 2017. However, the criticisms that are made are not criticisms that appear to us to suggest any serious systemic failure in relation to the approach of the Agencies to proportionality. Such understandable criticisms as have been made by the Claimant as, for example, that MI5 appeared to operate their searches on the basis of a default of sweeping all the data rather than seeking to introduce some alternative mechanism, have been addressed and explained in open and closed by the Respondents, and such criticisms may yet be accommodated. From what we have seen and heard in closed evidence, we accept that the Respondents are required to, and do, consider on each occasion whether there are less intrusive means of obtaining the information which can be derived from these databases quickly enough to serve the investigative and operational aims of the exercise. This remains in a state of development, and continuing discussion with the Commissioner. We have been reassured about how the databases are used, bearing in mind in particular, as we do, the wide margin of appreciation allowed to the Respondent in assessing its pressing social needs and achieving its legitimate aims of protecting national security (**Leander v. Sweden**

[1987] 9 EHRR 433 and **Lumsdon** at para.64). We are satisfied that consideration of proportionality is inbuilt into the Agencies' systems, and that there is regular consideration, at both the stage of acquisition and of access, of whether there are any practical alternative measures that could be taken.

94. In the circumstances which we have considered in open and in closed, we consequently resolve the issue of proportionality, reserved by paragraphs 16(d) and 102 of our First Judgment, in favour of the Respondents.

Issue 5: Setting Aside the First Judgment

95. The Claimant does not seek to set aside the whole of our First Judgment, but only that part of it which concluded in paragraphs 72 to 84 that:-

> (i) So far as concerned the BPD regime, during the period of Sir Mark Waller's supervision, independent oversight had been and continued to be adequate, but that for other reasons it failed to comply with the ECHR principles until March 2015.
>
> (ii) So far as concerned the BCD regime, supervision by the IOCC was adequate only after July 2015, but that the regime remained non-compliant with ECHR principles prior to its avowal in November 2015.

96. With regard to the adequacy of oversight, we set out our conclusions at length in that Judgment, after full consideration of the evidence. The Claimant seeks to persuade us to set aside our Judgment, so as to substitute a conclusion that the oversight of both regimes by both Commissioners remained inadequate, effectively until September 2017, when IPCO took over.

97. After consideration of the issues relating to s.94, other than those which we have considered in this Judgment, we concluded that the BCD regime and the directions made for BCD thereunder pursuant to s.94 were lawful, namely compliant with statute. As a result of our conclusions on Issue 1, our decision now is that in relation to many of the directions made by the Foreign Secretary pursuant to s.94 prior to October 2016, they were unlawful. The result is that so far as BCD is concerned, the period in respect of which we have concluded that the BCD system was lawful is now substantially deferred from November 2015 to October 2016. To that extent, therefore, on the one hand our Judgment, on those grounds, has thereby been reopened, and on the other hand the period in which the Claimant can seek to reopen our Judgment yet further is of very short duration.

98. As set out above, we concluded on 1 December 2017 that there was sufficient produced before us by the Claimant to permit its application to reopen to go forward, and we have not needed to consider at any length the legal basis by which we would reopen our Judgment, and there has not been any need to look at authorities. It is common ground between the parties that, if our Judgment was flawed, based upon materially inaccurate evidence, i.e. if evidence, which was material to our decision, was materially inaccurate, we would reopen the Judgment, at least to the extent of reconsidering the issues in the light of all the evidence. It is clear that no such reopening of a concluded Judgment would occur unless such material evidence was fresh evidence, that is evidence which neither was nor could reasonably have been known to the Claimant at the time of the original Judgment.

99. Sir Mark Waller was tasked to conduct statutory oversight of BPD across the three agencies in March 2015, although he had been conducting extra-statutory oversight of

BPD as from December 2010 in his bi-annual visits. Sir Anthony May was tasked to oversee BCD on an extra-statutory basis in February 2015. This is before the start of the relevant period (November 2015). Sir Stanley Burnton took up the job of IOCC on 4 November 2015 and produced a report on s.94 authorisations within 7 months. Sir Mark's report on 2015 was published in July 2016, but that is an annual report summarising his ongoing work during the whole year.

100. Sir Stanley Burnton identified the difference in scope between the submissions made by GCHQ to the Foreign Secretary and the authorisations he or she then granted and made a recommendation which resulted in new and lawful authorisations being granted in October 2016, less than a year after he was first appointed. The recommendations he made were substantially accepted by the Home Secretary in her letter of 17 January 2017.

101. Sir Stanley Burnton's inspectors then attended GCHQ in April 2017 and prepared a report on the s.94 authorisations, as we have explained above.

102. It follows from the above that there was a system of oversight by independent Commissioners in place throughout the relevant period, and the Commissioners had been specifically tasked to consider the use of bulk datasets.

103. The original basis for the application is set out in the Claimant's Application for Reconsideration of the October 2016 Judgment dated 10 November 2017, but it has been supplemented, and to an extent overtaken, by what has occurred since, during the course of what we have referred to above as the iterative nature of the applications and hearings before us. The grounds appear to us now to fall into four categories:-

(i) The s.94 Directions:

(ii) Sharing with industry partners:

(iii) The IS Comm's method of oversight:

(iv) Criticisms of the oversight by the previous Commissioners which can be spelt out of the recent correspondence with IPCO.

There are two other matters raised by the Claimant's Solicitors in their letter to the Tribunal dated 18 April 2018, subsequent to the last hearing, which the Tribunal has taken into account, relating to the 2015 and 2016 Confidential Reports of IS Comm.

104. Before considering whether there is ground for reopening the decision that the Tribunal made as to adequacy of oversight, we have decided to consider carefully the approach in paragraphs 68 and 69 above with regard to what is required in order to amount to adequate oversight, so far as we can form a view on the evidence before us.

105. If we were persuaded to reopen the Judgment, we would need to reconsider all of the earlier evidence as to supervision which we considered in detail before giving our First Judgment, together with any other admissible evidence, and in considering the new evidence we must look at it in the context of the old.

Section 94.

106. The issue for this purpose is whether Sir Stanley Burnton, the then IOCC, failed in his oversight when carrying out his July 2016 Review of the s.94 directions. He concluded in his July 2016 review, as we have discussed in relation to Issue 1, that the s.94 directions were inadequate, on much the same basis as we have concluded that they did not comply with the terms of s.94, although that was not his remit, and he recommended the steps which led to the new October 2016 direction. We have endeavoured to find out, with IPCO's help, a not altogether straightforward task for IPCO given the passage of time and the high classification of the documents,

precisely what documents were supplied to the IOCC's team in 2015-16, on the basis of which the conclusions in the July 2016 Review were arrived at. Mr de la Mare QC submits that there is effectively a Morton's fork: either the IOCC's team was not shown all the documents, whereas the GCHQ witness's evidence is as to his belief that they were, or the IOCC's team was shown all the documents and reached an inadequate conclusion. However, after our full reconsideration of the documents, we have concluded that, although the GCHQ witness did not give a clear description of what documents were shown to Sir Stanley, in fact it does appear that all relevant documents were made available to him, and that he reached conclusions with which we agree. We do not consider there is a Morton's fork. Given that Sir Stanley Burnton's conclusion was correct, and was complied with, and that we have concluded that, once the directions were sought and granted in their new form, the system became lawful as from October 2016, we do not conclude that there was any inadequacy of supervision by reference to the July 2016 Review.

Industry Partners

107. As we have set out in paragraphs 80 to 85 above, whereas it is apparent that the Commissioners knew of the use of contractors in-house, they did not know precisely how many such contractors were so employed, or in what positions. Although the use of such in-house contractors did raise a risk, the absence of such precise knowledge does not in our judgment detract from the adequacy of their oversight, which in this regard was in place and, so far as checking conduct by contractors as well as employees, was plainly exercised. What is however significant is that the Commissioners did not know about sharing with industry partners by GCHQ, as described in paragraphs 79 and 82 above. This is an area which has fallen under the

microscope of this Tribunal because of the reservation of the issue of sharing generally in our First Judgment, but it plainly forms a minimal part of the operation of BPD/BCD, and an even more miniscule part of the work of the Agencies subject to the Commissioners' oversight. This is a failing in the operation of oversight, and in the duty of GCHQ to bring it to the Commissioners' attention. However, given the totality of the work done both by the Commissioners and by the Agencies, we do not conclude that this amounts to or illustrates a systemic failure.

IS Comm

108. The Claimant has criticised IS Comm for not having a team of Inspectors, as did Sir Stanley Burnton, or obtaining independent technical advice. This does not seem to us in any event strictly to be fresh evidence, because much of the basis for the Claimant's criticism arose from what Sir Mark Waller himself said to Parliament in March 2014 and December 2015. But there is no doubt that he did carry out supervision, with diligence and regularity, and it can be seen by simply reading his reports how detailed he was in his consideration, and how many detailed and technical points he explored with the Agencies. His aim, as he explained it to Parliament, was to make sure that he had personal oversight, which was not delegated to others, and it is plain that he frequently required and received regular explanations. Another Commissioner might have taken a different view as to the appropriateness of technical assistance, but the perceptive nature of his comments in his reports, and the fact that he often required changes and improvements, show that he had, and was able to have, a hands-on approach, and we refer to paragraph 69 (iv) above.

109. In our judgment the fact that the new supervision regime now has the benefit of a team of experts, as a result of the statutory provision under the new Act, may be an

improvement, though it is not yet tested, but it does not, in our judgment, evidence prior inadequacy. Such criticism seems to have arisen as a result of what was said in the IPCO correspondence, but it is in any event met and addressed, and in our judgment rightly, by Sir Adrian Fulford's letter dated 28 November 2017 to which we have referred in paragraph 70 above; he includes numerous extracts from Sir Mark's reports, refers to the numerous technical briefings from the Agencies given to him, and makes the statement in relation to the approach by predecessor organisations, plainly including Sir Mark Waller, which we have there set out. In any event this argument, if there was any substance to it, could have been made to us prior to our First Judgment, in reference to Sir Mark's own statements, many months earlier.

IPCO correspondence

110. It is in that context that we approach the other matters drawn by the Claimant from the earlier IPCO correspondence. Responses to them were put before us in evidence from the Agencies by way of correction or amplification, and we are in no position to resolve those issues, such as they are, certainly in the confine of an application to set aside our fully reasoned Judgment. Reference was made by the Claimant, as referred to in paragraph 93 above, to 'amber warnings' given by IPCO in the course of an inspection of GCHQ in April 2017, which were said to be intended to lead to a *"development* [which] *will enhance the oversight given by the Commissioner"*. Such criticisms do not in our judgment undermine, but rather exemplify, the nature and adequacy of ongoing oversight. There is a dispute about whether search terms were only made available on request, as opposed to being supplied without request, as they were apparently from June 2017 onwards. In a draft September 2017 IPCO report (to which we have already made reference) "*GCHQ demonstrated that they had*

considered the necessity and proportionality of any sharing that might take place … however it was felt that GCHQ fell short of providing IPCO complete assurance of their compliance in some areas".

111. We have no doubt that, just as the previous Commissioners pointed out errors by the Agencies, and just as the Agencies themselves produced some incorrect evidence to us, to which we have referred above, there have been continuing mistakes and lacunae, some of which have been picked up, but some of which no doubt have not been picked up over the period of years. We however remain of the view that there is no basis for reconsideration of the conclusions we reached as to adequacy of oversight in our First Judgment. There is and has been a genuine determination both on the part of the Commissioners and the Agencies themselves to get things right. As we said at the outset of this Judgment, the very involvement of this Tribunal, which has in this case been stimulated and prompted by the diligence and hard work of the Claimant, contributes towards an ever increasing improvement in the safeguards without, it is to be hoped, endangering the vital work which the Respondents are carrying out. The reopening of a judgment is in any event a matter of discretion, and it is significant that the oversight regime has now been replaced by an entirely new system.

112. We dismiss the application to set aside the conclusions in our First Judgment in relation to the Commissioners.

Outcome

113. We conclude as follows:-

Issue 1 and 2:

We unanimously conclude that those Directions by the Foreign Secretary identified in the CLOSED schedule were not in accordance with the law, but we make no further order.

Issue 3A:

By a majority we conclude that the regime in respect of sharing of BCD/BPD with foreign agencies complies with Article 8 ECHR.

Issue 3B:

We unanimously conclude that the regime in respect of sharing BCD/BPD with law enforcement agencies complies with Article 8 ECHR and UK domestic law.

Issue 3C:

We unanimously conclude that the regime in respect of sharing BCD/BPD with industry partners complies with Article 8 ECHR.

Further, in relation to GCHQ's avowed sharing of BCD/BPD with industry partners, we unanimously conclude that such sharing was compatible with Article 8 ECHR.

Issue 4:

We unanimously conclude that the steps taken by way of collection, retention and use of BCD or BPD by the Respondents comply with the requirements of proportionality pursuant to Article 8 ECHR and EU law.

Issue 5:

We unanimously conclude that, save in the respect consequent upon our conclusion in relation to issues 1 and 2, the application to set aside the conclusions in our First Judgment is dismissed.

———————

APPENDIX 1 TO JUDGEMENT OF 23 JULY 2018 (as substituted on 26 July 2018)

OPEN INTRODUCTION TO CLOSED JUDGMENT

1. The closed part of the Judgment is in two parts

   Part 1: The closed section relating to the s.94 directions referred to in paragraph 53 of the Open Judgment where the function of this section is fully explained;

   Part 2: The closed section dealing with sharing of BCD/BPD and oversight of any such sharing.

2. In accordance with its legal obligation, the Tribunal has conducted as much of its proceedings in public as is possible, and will publish as much of its conclusions as is possible. Just as some of those proceedings were closed, so also it is intended to produce a closed judgment.

3. The questions now under consideration are whether the UKIC may lawfully share such bulk datasets with

   a. The security services of foreign powers ("foreign partners");
   b. Corporations and individuals with whom the UKIC may contract for the provision of services ("industry partners");
   c. Law Enforcement Agencies (LEAs) within the UK, for example HMRC or the police.

4. The Respondents do not confirm or deny that any such sharing has ever taken place or that it is contemplated. The Tribunal accepts that this is a lawful stance for them to take and proceeds on that basis. Nothing in this Judgment addresses what has actually

happened or which may actually happen. The open part of the Judgment proceeds on the assumption that such sharing may take place and considers

a. the legal test which should be applied before it could lawfully happen,
b. the safeguards which should be in place to render it lawful; and
c. the oversight regime which would ensure that (a) and (b) were effectively complied with.

5. This case does not concern the product of an investigation by the UKIC using BCD/BPD. That product will no longer be bulk data, but will be intelligence capable of being actioned like any other such intelligence. The sharing under consideration here is the sharing of "raw data". It does not follow from this that any such sharing must inevitably involve the sharing of the whole dataset because a degree of editing or filtering is conceivable which might reduce the intrusiveness of any such sharing. A dataset which has been filtered in this way, but which remains a bulk dataset, is sometimes called a "sub-set" in the documents.

<u>The open parts of the hearings</u>

6. The Tribunal has received open submissions from the Claimant based on certain aspects of sharing which have entered the public domain, and on inferences which have been drawn from material within their knowledge. Sometimes those inferences have the appearance of speculation, but in this context that is not a matter of proper criticism for obvious reasons. What is publicly known is that

a. Sharing of intelligence generally (as opposed to BCD/BPD in particular) has taken place with foreign partners. From this it is suggested that it is at least possible that the UKIC may at some stage contemplate sharing of BCD/BPD

and therefore that the lawfulness of such a step is not a merely theoretical issue.

b. There is a degree of access by industry partners to UKIC sites and systems. The UKIC must commission systems from external developers and manufacturers and for that purpose it is inevitable that they must work with such organisations and people.

c. In particular, GCHQ has a relationship with Bristol University which is in the public domain. The arrangement with Bristol University is that the Heilbronn Institute for Mathematical Research has a partnership arrangement with GCHQ. It uses GCHQ systems and the data does not leave those systems. The Director is a member of GCHQ staff and other GCHQ staff provide management and supervision of its operations. This may look like sharing with an external body, but in fact it is not. A minority only of the academic researchers have access to data derived from a sensitive database. That access is limited to operational data which has been narrowly focussed, which has remained under GCHQ control, which has been subject to full legal safeguards and which is restricted to GCHQ systems. In the form in which such access occurs, the data is no longer a bulk dataset.

A principal purpose of the work of parts of the UKIC is the supply of intelligence to LEAs. The power in s.19 CTA, see paragraph 73 of the open Judgment, exists in order to extend that activity to all material legitimately acquired by the UKIC even where it was acquired for one purpose and is shared for another. We accept that we should examine the contention that the UKIC may wish to supply raw BCD/BPD (as opposed to product) to LEAs as part of this activity as a hypothetical assumption.

7. The Claimant relies on the evidence of Dr. Gus Hosein (see paragraph 81 of the Judgment) which points to risks which have been identified in other spheres of activity where organisations have allowed access to, or control of, their systems to external bodies. We have borne that evidence in mind when reaching our conclusions. Commercial organisations such as those described by Dr. Hosein cannot rely on the criminal law to secure compliance by staff and contractors to the same extent as UKIC, and do not operate the same system of vetting of staff and contractors as is operated by the UKIC. The Tribunal concludes that it is these systems and controls which are critical in assessing the level of risk in permitting access, and accordingly the evidence of Dr. Hosein of how other organisations, which are less well protected in other ways, proceed is not decisive. The risk of negligent or malign misconduct by directly employed staff or external contractors cannot be excluded. The question is whether it is limited as far as reasonably possible by appropriate management.

8. The GCHQ witness was cross-examined about some of these issues in open, and the Claimant's submissions were informed by that exercise. That was an exceptional step taken by the Tribunal because of the concerns about his evidence dealt with in the open Judgment. The Claimant submitted that the Tribunal should conclude that external contractors always pose a higher risk than directly employed staff from the fact that Edward Snowden was not directly employed by the NSA at the time when he extracted and removed data. This contention was explored with the GCHQ witness in his evidence in open session and he replied that he did not accept it.

9. In relation to oversight, the Claimant was able to rely on the published reports of the Commissioners (ISCom and IOCC), who had that task prior to IPCO's inauguration on 1 September 2017. The relevant period in the light of the findings in the First Judgment is 4 November 2015- 31st August 2017 ("the relevant period"). Before that, the acquisition of BPD and BCD has been held unlawful already in the First Judgment. The Claimant also relied on correspondence and minutes and reports of inspections by IPCO, in this context as well as in support of the application to re-open in part the First Judgment.

10. In response to these submissions the Respondents made some submissions in open, but also made submissions in closed. The Tribunal heard evidence in closed and was assisted in that process by Mr. Glasson QC, Counsel to the Tribunal. Afterwards, Mr. Glasson assisted further by opening up and disclosing as much of what had been said in closed as was possible, which further assisted the Claimant in refining its submissions. Mr. Glasson was acting in these respects as Counsel to the Tribunal, but in a capacity which is independent of the Tribunal, and he is free to make such submissions as he considers necessary to ensure that the claim is fairly dealt with.

<u>The approach of the Tribunal</u>

11. The Tribunal considers that transparency is a prime consideration in dealing with claims of this kind. It is accepted by the Claimant, as it clearly must be, that full disclosure would defeat the object of the existence of the UKIC and endanger the security of the nation. Transparency must therefore be curtailed as far as is necessary, but only so far. We have endeavoured to achieve this goal and in that endeavour have engaged in a long and careful series of hearings, with extensive consideration between them of what must remain closed.

12. As far as possible, our conclusions on sharing and on the related question of re-opening the First Judgment on oversight are set out in the Open Judgment at paragraphs 61 to 85 and 95 to 111. The Tribunal has also prepared the Closed Judgment which determines the Claimant's submissions by reference to the evidence heard in closed session. The function of that Judgment is to inform those who can have access to it of our findings, and it will play its part in assisting the UKIC and IPCO in the process of constant improvement which is, or should be, inherent in any effective system of oversight. The fact that the Tribunal has prepared a reasoned decision on the evidence and submissions which it heard in closed should operate as a reassurance to the Claimant that their claims have been taken seriously and investigated by an independent Tribunal with the assistance, as we have said, of independent Counsel. The Tribunal did so on the basis of evidence given on oath or under affirmation. That is an important guarantee of honesty and reliability.

CONCLUSION:

13. The conclusion of the Tribunal, unanimous as to all issues save Issue 3A as set out in the Closed Judgment, is that since 5th November 2015 (14th October 2016 in respect of Issue 1) there are no systemic failures in the arrangements for the acquisition and use by UKIC of BCD/BPD or in the oversight regime which render any sharing unlawful, and that there is no basis to reopen the First Judgment, save as to the conclusions on Issue 1. In certain respects, the evidence adduced before the Tribunal has given rise to serious concerns which are addressed in the Closed Judgment. The conclusions of the Tribunal set out in the Open Judgment are consistent with its conclusions in the Closed Judgment. In respect

of Issue 3A, each of the dissenting Members has set out reasons for such dissent as annexures to the Closed Judgment.

14. The re-opening of a Judgment is a matter of discretion and we have reached our decision to refuse to do so for the reasons set out in paragraphs 95-112 of the Open Judgment and because

    a. The concerns affect an oversight regime which has now been replaced by an entirely new system. The IPA provides a new code for decision making in this area. IPCO has replaced the Commissioners whose effectiveness is in issue in this case.

    b. There is no evidence that any failings of oversight have in fact resulted in any unlawful use of data. We have not identified any person to whom a remedy should be granted.

    c. The failings concern only a limited area of one agency.

    d. The failings are now under the active scrutiny of IPCO which is fully aware of the matters of concern at GCHQ and which has the capacity to ensure that they are remedied.

    e. Our inquiry has involved a degree of re-opening of the conclusion and we are satisfied that no substantial benefit will accrue from any further consideration of these issues in the present context.

    f. The exercise which we have now conducted has involved a historical investigation which has produced valuable information which will inform future decision making by GCHQ and oversight by IPCO. We offer some observations on the evidence in the last part of the CLOSED Judgment which we hope will assist in that exercise. We consider that this adequately addresses what has been discovered, without re-opening the whole of the evidence which resulted in the First Judgment.

15. The conclusions of the Tribunal set out in the Open Judgment are consistent with its conclusions in the Closed Judgment. In respect of Issue 3A, each of the dissenting Members has set out reasons for such dissent as annexures to the Closed Judgment. The majority share concerns expressed in those dissenting opinions though the majority does not accept that they are a sufficient basis to affect our conclusion that the regime in respect of sharing BCD and BPD was compliant with Article 8.

16. The Tribunal has examined and determined the issues of the basis of the claim as it has been advanced. This is essentially a claim based on Article 8 rights of persons whose data has been acquired by UKIC as part of bulk datasets. It relates to a previous and superseded regime of oversight. This case concerns bulk datasets and Article 8 and our conclusions are made in that context.

17. The issue of foreign sharing of intelligence more generally is a matter of the greatest importance. The risk that a partner state may use intelligence from UKIC in a way which would be unlawful is a subject of concern, and may give rise to consideration of Articles 2 and 3 in addition to Article 8. Similarly, sharing of bulk datasets with a commercial or political organisation which might misuse them for commercial gain or political advantage is one which gives rise to a need for rigorous control and oversight. Nothing in our conclusions understates the importance of proper management and oversight of these potentially hazardous activities. The Tribunal has no reason to suppose that IPCO takes any different

view and confidently expects vigorous oversight of any such activities in future, whether they arise in the bulk dataset context or otherwise.

APPENDIX 2 TO JUDGEMENT OF 23 JULY 2018

Handling Arrangements and other guidance in relation to sharing BPD/BCD outside the SIA

Double-underlining within extracts indicates gisting.

Statutory safeguards

1) The regime in respect of Bulk Personal Datasets ("BPD") and Bulk Communications Datasets ("BCD") which is relevant to sharing by the Intelligence Services with foreign liaison/LEAs/industry partners principally derives from the following statutes:

   a) the Security Services Act 1989 ("the SSA") and the Intelligence Services Act 1994 ("the ISA");

   b) the Counter-Terrorism Act 2008 ("the CTA");

   c) the Human Rights Act 1998 ("the HRA");

   d) the Data Protection Act 1998 ("the DPA"); and

   e) the Official Secrets Act 1989 ("the OSA").

2) There are also important **oversight mechanisms** in the regime provided by the Interception of Communications Commissioner and the Intelligence Services Commissioner (both of whom were replaced, on 1 September 2017, by the Investigatory Powers Commissioner) and by the Intelligence and Security Committee and the Tribunal. These mechanisms have already been considered and approved by the Tribunal in its October 2016 judgment. However, the Commissioners' role in relation to disclosure/sharing of BPD/BCD is addressed below.

The SSA and ISA

Security Service functions

3) By s.1(2) to (4) of the Security Service Act 1989 ("SSA"), 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."

4) 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

5) By s.1(1) of the ISA, 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."

6) 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."

7) 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

8) By s. 3(1)(a) of the ISA, 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 ...."

9) 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."

10) 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 ...*"

11) 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

12) 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."*

13) 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*."

14) 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))

15) 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)."

16) 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)."

17) 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.

The HRA

18) 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."

19) By s. 6(1):

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

20) 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/BCD-related activity, the HRA applies at every stage of the process i.e. authorisation/acquisition, use/access, disclosure, retention and deletion.

21) 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

22) 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."

23) 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.

24) 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]

25) 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

[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.

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

26) 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).

27) 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).

BULK PERSONAL DATASETS

Cross-SIA Policy

28) The Joint SIA BPD Policy, which came into force in February 2015 sets out agreed policy for each of GCHQ, the Security Service and SIS for sharing BPD:

> "**D. Sharing**
>
> All three Agencies have a common interest in acquiring and interrogating BPD. As a principle, all three Agencies will seek to acquire once and use many times, on the grounds of business effectiveness and efficiency. The following policy statements apply to the Agencies:
>
> When sharing BPD the supplying Agency must be satisfied that it is necessary and proportionate to share the data with the other Agency/Agencies; and the receiving

Agency/Agencies must be satisfied that it is necessary and proportionate to acquire the data in question. A log of data sharing will be maintained by each agency;

The sharing of BPD must be authorised in advance by a senior individual within each Agency, and no action to share may be taken without such authorisation;

Agencies must protect sensitive datasets (or certain fields within a dataset) when sharing, if the risk or intrusion in doing so is not judged to be necessary or proportionate;

BPD must not be shared with non-SIA third parties without prior agreement from the acquiring Agency;

Were BPD to be shared with overseas liaison the relevant necessity and proportionality tests for onwards disclosure under the SSA or ISA would have to be met. In the event that one (UK) Agency wished to disclose externally a dataset originally acquired by another Agency, Action-On would have to be sought in advance from the acquiring Agency. Wider legal, political and operational risks would also have to be considered, as appropriate..."

29) The OPEN BPD Handling Arrangements which came into force in November 2015 address disclosure of BPD at §§5.2, 6.1-6.7 and 8.1:

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

"6.0 Procedures and Safeguards for Disclosure of Bulk Personal Datasets outside the relevant Intelligence Service

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.

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.

6.4 Before disclosing any bulk personal data, staff must take reasonable steps to ensure that 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 that they have received satisfactory assurances from the intended recipient organisation with respect to such arrangements.

6.5 These conditions must be met for all disclosure, including between the Intelligence Services.

6.6 These conditions for disclosure apply equally to the disclosure of an entire bulk personal dataset, a subset of the dataset, or an individual piece of data from the dataset.

6.7 Disclosure of **the whole (or a subset) of a bulk personal dataset** is subject to internal authorisation procedures in addition to those that apply to an item of data. 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."

30) In addition:

"8.1 The acquisition, retention and disclosure of a bulk personal dataset is subject to scrutiny in each Intelligence Services 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."

Action On Process

31) Any data shared with other organisations would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance, or approved through the Action-on process. Action-on is a process which is used by each of the SIAs.

Commissioner oversight

32) By the Intelligence Services Commissioner Additional Review Functions (Bulk Personal Datasets) Direction 2015, the Prime Minister, pursuant to his power under s.59(a) of RIPA, directed the Intelligence Services Commissioner to *"continue to keep under review the acquisition, use, retention and* ***disclosure*** *by the* [SIAs] *of bulk personal datasets, as well as the adequacy of safeguards against misuse."* and to *"assure himself that the acquisition, use, retention* ***and disclosure*** *of bulk personal datasets does not occur except in accordance with"* the relevant sections of the SSA 1989 and ISA 1994 and to *"seek to assure himself of the adequacy of the [SIAs'] handling arrangements and their compliance therewith."* (emphasis added)

33) Before 1 September 2017, the Intelligence Services Commissioner had oversight and access to all SIA material in relation to BPD/BCD compliance, including that relating to sharing. For the avoidance of doubt, that would extend to any activity of the SIA, were it to take place, relating to BPDs, including sharing with partners or giving partners remote access. In answer to a request by the Tribunal dated 13 April 2017 about what he regarded as within his remit the Intelligence Services Commissioner confirmed, by a letter to the Tribunal dated 27 April 2017 written jointly with the Interception of Communications Commissioner, that both "use" and "disclosure" are *"taken to include sharing with other agencies or organisations, including foreign agencies."* Since 1 September 2017 the Intelligence Services Commissioner's functions have been performed by the Investigatory Powers Commissioner.

Breaches of safeguards

34) In the event that any of the SIAs' policies and safeguards in respect of sharing BPD were breached, the relevant Agency would report any such breach to the Intelligence Services Commissioner (or now the Investigatory Powers Commissioner); investigate the breach; consider whether it remained lawful or appropriate to continue to share; if and to the extent that any Agency staff had committed the breach in question, consideration would be given to disciplinary proceedings.

GCHQ

35) Section 9 of the GCHQ BPD Handling Arrangements which came into force in November 2015 addresses disclosure of BPD at section 9:

> "**9. Disclosure**
> 9.1 Where the results of bulk personal data analysis are disclosed to partner or customer organisations, this must be done via standard reporting mechanisms, which ensure release of GCHQ intelligence in a secure, accountable, legally compliant manner.
> 9.2 If disclosure of a bulk personal dataset, or a substantial part of it, to a partner organisation is contemplated, whether at GCHQ's or the partner's initiative, the procedures below must be followed:
> ...
>
> [REDACTED]
> 9.4 Other organisations:
> 9.4.1 For any other organisation, whether another UK partner or a *foreign partner*, the dataset's Requester or Endorser will submit a request for authorisation to disclose, by means of the dataset's BPD form. Again, such requests will be considered by *relevant GCHQ senior officials*.
> 9.5 All requests for authorisation to disclose must provide a persuasive justification for the proposed disclosure, in terms of:
> – its necessity and proportionality, and
> – the intelligence or other operational benefit that is expected to accrue to GCHQ and the UK from the disclosure.
> 9.6 The Authoriser will consider:
> – the content of the dataset: the nature of the personal information it contains, its intrusiveness and sensitivity;
> – the nature and extent of the corporate risk the disclosure would entail;
> – the necessity and proportionality of the disclosure, including whether it is genuinely necessary and proportionate to disclose the whole dataset, or whether a subset will meet the need;
> – whether any caveats or restrictions should be applied; and
> – the receiving organisation's arrangements for safeguarding, using and deleting the data – GCHQ will seek additional reassurances from the receiving organisation in this regard, if the Authoriser deems it necessary."

36) The form referred to at §9.4.1 of the GCHQ BPD Handling Arrangements is GCHQ's Bulk Personal Data Acquisition Retention (BPDAR) form, which, *inter alia*:

a) Requires the necessity and proportionality case for sharing BPD to be set out *"if it is proposed to share some or all of [the] dataset with an external organisation other than that which provided the data to GCHQ in the first place."* ; and

b) Requires identification of whether the BPD contains any sensitive personal data, and if so what kind .

GCHQ Policy on sharing BPD with foreign liaison/LEAs

37) GCHQ operates on the basis that operational data of any sort may only be shared if it is necessary for one of GCHQ's statutory functions, and, as far as GCHQ's intelligence gathering function is concerned, in line with one of the three purposes for which that function can be exercised. This is set out in GCHQ's Compliance Guide. All sharing is subject to compliance with all relevant legal safeguards, and there is a requirement that recipients must accord the material a level of protection equivalent to GCHQ's own safeguards. The assessment of whether a partner's safeguards meet this standard is a matter for the Mission Policy team, in partnership with departmental legal advisors and other specialist teams as appropriate. As a matter of policy GCHQ applies the safeguards required by RIPA to all operational data even if was not obtained under RIPA powers, so this is the standard that must be met. Sharing is also subject to policy approval by an appropriately senior member of the Mission Policy team, unless an explicit delegation of approval authority has been made. Policy approval may be subject to appropriate filtering or sanitisation of the data being applied to protect sensitive material or equities.

38) The Compliance Guide makes clear that, in line with the RIPA Interception of Communications Code of Practice, particular consideration should be given in cases where confidential information (which includes, inter alia, material that is legally privileged, and confidential journalistic information) is involved. Special care must be taken to ensure that the acquisition, analysis, retention and dissemination of such material is necessary and proportionate. This covers any sharing of such data with partners. Any sharing of BPD in whole or in part is subject to formal approval by Deputy Director Mission Policy who will take into account the potential for such data to contain confidential information and ensure that this is removed from the data to the extent possible (e.g. by the removal of particular fields from datasets) and will require the application of additional or more stringent safeguards where appropriate.

39) Were GCHQ to share BPD with foreign liaison or LEAs, then it would:

a) Follow the principles and approach set out in their respective Handling Arrangements and policy/guidance.

b) Take into account the nature of the BPD that was due to be disclosed.

c) Take into account the nature/remit of the body to which they were considering disclosing the BPD.

d) Take into account the approach taken by any other SIAs who may have shared bulk data and have regard to any protocols/understanding that the other agencies may have used/followed.

e) Depending on the individual circumstance, seek assurances that the BPD in question would be handled in accordance with RIPA safeguards i.e. that it would be disclosed, copied, distributed and retained only to the minimum extent necessary for the purposes of RIPA (in the interests of National Security, for the purpose of preventing or detecting Serious Crime, or for the purpose of safeguarding the economic well-being of the UK.

40) In addition, were GCHQ to give liaison partners and/or law enforcement agencies remote access to run queries to BPD, it would apply safeguards which would put partner analysts on the same basis as GCHQ analysts. In particular, GCHQ would:

a) Require analysts to have completed all relevant training (including legalities training), be assessed as having sufficient analysis skills, and to have all necessary nationality and security clearances;

b) Require all queries to be accompanied by necessity and proportionality statements which would be subject to audit by GCHQ;

c) Require analysts to comply with GCHQ's Compliance Guide and other BPD policies and safeguards concerning access, retention and use (as set out in the Cross-SIA and GCHQ BPD Handling Arrangements);

d) Comply with the safeguards regarding the treatment of LPP and journalistic material addressed in the required training and the Compliance Guide.

<u>GCHQ policy on sharing BPD with industry partners</u>

41) GCHQ may share operational data with industry partners for the purpose of developing and testing new systems. Actual operational data would only be shared for such purposes if it were not possible to use standardised corpuses of non-operational data. Any sharing would be of the minimum volume of data necessary to develop or test the system. In all cases the data would be the least intrusive data that can serve the purpose. For this reason any data known or believed to contain confidential information would not be used; similar data that does not contain such material would be used instead. Wherever possible data shared with industry partners will be held on GCHQ premises, where most systems development takes place, failing that the data must be

held on secure and accredited corporate premises in the UK. All sharing of data with industry is recorded on a Raw Data Release Request form which must be completed by a member of GCHQ who is sponsoring the activities of the industry partner. This form (which is used for certain other forms of data sharing which do not involve BPD) requires the sponsor to describe the purpose of the sharing and the details of the data they wish to release. If the data is to leave GCHQ premises they must specify where it is to go, and how it will be transferred. The form requires the sponsor to detail the name, organisation and job title of the individual who will take responsibility for the data on receipt, how many people at the recipient organisation will have access, for how long the data will be retained and what will be done with it once the project is completed. These requests are assessed within the Mission Policy team and may be escalated up to the Deputy Director Mission Policy where appropriate. Mission Policy will assess each proposal to ensure that the sharing is both necessary and proportionate, and may require modification of the request if there are concerns about proportionality.

Security Service

42) The MI5 BPD guidance of March 2015 addressed sharing/disclosure of BPD as follows:

> "Sharing Bulk Personal Data
> The sharing of BPD is carefully managed to ensure that disclosure only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The decision to share a BPD outside the Security Service rests with *a senior MI5 official* on behalf of DSIRO.
>
> Sharing within the SIA
> To the extent the SIA all have a common interest in acquiring information for national security purposes, it may be lawful for MI5 to share BPD with SIS or GCHQ. Within the SIA, the relevant gateways for these purposes are (i) section 2(2)(a) as far as disclosure by the Security Service is concerned, and (ii) sections 2(2)(a) and 4(2)(a) respectively of Intelligence Services Act so far as acquisition by SIS and GCHQ are concerned.
>
> In relation to each dataset, there are two sides to the information transaction, whereby both the disclosing and receiving agency have to be satisfied as to the necessity and proportionality of sharing a particular dataset. MI5 need to establish in each case that both (i) disclosure by the Security Service under section 2(2)(a) is necessary for the proper discharge of the Security Service's statutory function of protecting national security, and also (ii) that acquisition by SIS and GCHQ is necessary for their respective statutory functions in respect of national security under sections 2(2)(a) and 4(2)(a) respectively of ISA.
>
> In circumstances where GCHQ or SIS identifies a requirement, they should discuss their requirements with the relevant MI5 data sponsor. If the requesting agency and the MI5 data sponsor believe there is a business case to share the data a formal request must be made to

MI5 via *a relevant form*. [REDACTION] The relevant data sponsor is then responsible for submitting *the relevant form*.

The relevant form

The relevant form outlines the business case submitted by the requesting Agency, detailing the data requested, the necessity and proportionality case for disclosure of that data and the proposed data handling arrangements. This must be approved by the relevant data sponsoring *senior MI5 official* before being submitted to *the relevant team* who will consult *a legal adviser* on the legality of disclosure and the relevant technical feasibility.

A senior MI5 official will confirm the strength of the business case for sharing data is sufficient, and any security, ethical and reputational risks have been adequately considered. [REDACTION]

Once *the relevant form* is approved by *a senior MI5 official*, arrangements will be made for the data to be shared with the relevant Agency using suitably accredited network for electronic transfer. Where electronic transfer is not possible, physical transfer must be conducted in accordance with policy."

"Sharing outside the SIA

MI5 neither confirms, nor denies the existence of specific BPD holdings to organisations outside the SIA or a limited number of individuals within OSCT. Therefore any request to share BPD with an organisation other than GCHQ or SIS should reiterate this position as the requestor should approach the provider themselves. Attempts to ascertain MI5 BPD holdings by non-SIA organisations should be reported to *the relevant team*.

In the event that a formal request is made to MI5 for BPD to be shared, the same legal disclosure tests would need to be applied as when sharing with BPD partners. The requestor would also require a legal gateway to acquire the data, which the Security Service would need to be satisfied met the test of necessity and proportionality. All enquiries should be directed to *the senior MI5 official*."

43) The Security Service BPD Handling Arrangements which came into force in November 2015 address disclosure outside the SIA in section 6:

"**6.0 Disclosure**

6.1 The disclosure of BPD is carefully managed to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The decision to share a BPD outside the Security Service rests with a *senior MI5 official*."

"6.2.1...Information in BPD held by MI5 can only be disclosed to persons outside the Service if the following conditions are met:

- that the objective of the disclosure falls within MI5'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.

6.2.2 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the BPD is 'really needed' for the purpose of discharging a statutory function of MI5. 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 data.

6.2.3 The disclosure of the BPD 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 MI5's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved.

6.2.4 These conditions must be met for all disclosure, including between the Intelligence Services. They apply equally to the disclosure of an entire BPD, a subset of the dataset, or an individual piece of data from the dataset.

6.2.5 Disclosure of **the whole (or a subset) of a bulk personal dataset** is subject to prior internal authorisation procedures in addition to the requirements in 6.2.1-6.2.3 above. Where these requirements are met, the BPD is formally requested by the requesting Agency from MI5 through an agreed disclosure procedure using *the relevant form*. The relevant data sponsor is then responsible for submitting *the relevant form* that will seek authorisation within MI5.

6.2.6 The *relevant form* outlines the business case submitted by the requesting Agency, detailing the data requested, the necessity and proportionality case for disclosure of that data and the proposed data handling arrangements. Disclosure of the whole BPD (or subset thereof) is only permitted once such authorisation has been given under this process. Once the authorisation has been given, arrangements will be made for the data to be disclosed to the relevant acquiring Agency."

"**6.3 Disclosure to liaison services**

6.3.1 [REDACTION]

6.3.2 There are however some circumstances, such as a pressing operational requirement, where disclosure to a liaison service [REDACTION] may be necessary and proportionate in the interests of national security. In this event, the same legal disclosure tests would need to

be applied as when disclosing to SIA partners, and *the relevant form* would have to be completed. MI5 would need to be satisfied that disclosure to the relevant liaison service met the dual tests of necessity and proportionality. All enquiries should be directed to *the data governance team*. Prior to disclosure, staff must (a) take reasonable steps to ensure that the liaison partner has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data (including with regard to source protection and the protection of the privacy of the individuals in the BPD) and ensuring that it is securely handled, or (b) have received satisfactory assurances from the liaison partner with respect to such arrangements."

44) The "relevant form" referred to at §§6.2.5, 6.2.6 and 6.3.2 of the Security Service BPD Handling Arrangements is the "Form for Sharing". It contains, *inter alia*, provision for:

a) Considering whether the BPD contains sensitive personal data, including but not restricted to journalistic and legally privileged material

b) Access restrictions: the *"arrangements agreed to ensure material is handled securely and what access control will be applied"* must be stated

c) Agreed caveats in relation to the handling of the material must also be set out

d) The "Business Justification & Privacy Assessment" requires the statutory purpose and a necessity and proportionality assessment to be set out, and approved by a senior MI5 official.

e) The technical feasibility of disclosure must be approved by the relevant technical team

f) Legal approval for disclosure must also be given by a legal adviser.

g) Final approval must also be given by DSIRO or designated person

Security Service Policy on sharing BPD with foreign liaison/LEAs/industry partners

45) Were the Security Service to share BPD with foreign liaison or LEAs, then it would only share if satisfied that:

a) Such sharing was for one of the Security Service's statutory purposes, or one of the limited additional purposes set out in s.2(2)(a) of the Security Service Act 1989.

b) It is necessary to disclose the information in question in order to achieve that objective;

c) That the disclosure would be proportionate to the objective;

d) That only as much of the information will be disclosed as is necessary to achieve that objective.

e) As set out at §6.3.2 of the Security Service BPD Handling Arrangements, the Security Service would also (a) take reasonable steps to ensure that the liaison partner has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data (including with regard to source protection and the protection of the privacy of the individuals in the BPD) and ensuring that it is securely handled, or (b) have received satisfactory assurances from the liaison partner with respect to such arrangements.

46) In the event that MI5 were considering sharing or were to share bulk data, then the approach that it would take, and the principles that it would apply, would be as described below.

47) The principles and approach that it would apply can be summarised as follows:

a) An information gathering exercise would be conducted in relation to the proposed recipient.

b) If that was satisfactory, then a sharing agreement would be prepared, if deemed necessary, to reflect the matters that MI5 considered (having regard to the information gathering exercise) needed to be covered.

c) Individual consideration of each bulk dataset to be shared would be carried out. If agreed, then any sharing of bulk datasets would be accompanied by specific handling instructions, setting out any particular requirements considered appropriate.

d) Ongoing review of the sharing relationship would be conducted.

<u>Stage 1 – information gathering</u>

48) In advance of initial sharing, and to inform the decision-making process to do so, an information gathering exercise would be undertaken to better understand the legal framework, policy and practice of the recipient. Specifically this exercise would gather information in the following areas which would inform decision making and any written agreements that were deemed appropriate:

a) Law and Policy – identifying the legal and policy regime that would apply in relation to bulk datasets in the recipient.

b) Acquisition of Bulk Data – identifying (if any) the process which would be applied before the recipient acquires bulk datasets and whether there is any legal and/or policy obligation to consider the necessity and proportionality of acquiring a particular dataset.

c) Authorisation – identifying the process and requirements (if any) that would be applied to authorise the retention and examination of bulk datasets.

d) Ingestion and Access – identifying how shared data would be stored, any categories of data the recipient considers sensitive (for example legal professional privilege) either by law or policy and any policy governing access to the raw dataset or intelligence derived from it.

e) Exploitation and Analysis – make reasonable enquiries regarding the use that would be made of the bulk data and the capabilities of the systems on which it would be used.

f) Disclosure – identifying any ACTION ON procedures or safeguards and the considerations taken into account when deciding to share bulk data with others.

g) Retention and Review – identifying the process and parameters by which the necessity and proportionality case for continuing to retain and exploit bulk data would be reviewed.

h) Oversight – identifying what internal and external oversight arrangements would be in place to audit the acquisition, retention and exploitation of bulk data.

49) In addition, in the event of any sharing of bulk data outside the SIA, MI5 would ensure that sharing of that data is in accordance with any wider HMG policies which MI5 is required to adhere to (for example HMG Consolidated Guidance).

Stage 2 – Sharing agreement

50) Subject to MI5 being satisfied following its information gathering exercise, a written agreement would, if considered necessary, be agreed between the recipient and MI5 in advance of any bulk data sharing. Insofar as considered appropriate, MI5 would require the recipient to apply

safeguards to the handling of any shared bulk data which correspond to MI5's domestic requirements. A written agreement may detail (taking into account the results of the information gathering exercise) requirements for the following aspects of sharing:

a) How shared data will be stored, accessed and used.
b) An agreed security classification for the shared data.
c) Suitable technical and organisational measures to protect data from accidental or unauthorised disclosure or misuse.
d) A requirement that permission be sought from the disclosing partner prior to any onward disclosure from the recipient of all or part of a bulk dataset or any targeted data derived from it.
e) A requirement that permission be sought from the disclosing partner prior to any executive action being undertaken by the recipient on the basis of any shared data or targeted data derived from it.
f) A requirement that disclosure of and access to any shared data be limited to appropriately cleared personnel within the recipient who have a business justification for access to the data.
g) All staff within the recipient with access to the shared data will be made aware of the provision governing the retention and examination of the shared data made within the written agreement.
h) A requirement for the destruction of the shared data as soon as its retention is no longer deemed to be necessary or proportionate.
i) A requirement to inform the disclosing partner of any threat to life reporting obtained from examination of the shared data.
j) An assessment that the sharing of data complies with the disclosing partner's legal obligations and that the receipt of the data by the receiving partner complies with their legal obligations.

<u>Stage 3 – Individual consideration of each bulk dataset to be shared and the terms of handling instructions to accompany each bulk dataset shared</u>

51) In every instance where sharing of bulk data were proposed then there would need to be particular consideration of that proposed sharing, having regard to the terms of any sharing agreement in place. In each case where a bulk dataset were shared with a partner, specific handling instructions would accompany it. In addition, insofar as considered appropriate, MI5 would require the recipient to apply specific safeguards to the handling of any shared bulk data which correspond to MI5's domestic requirements appropriate to the nature of the data being shared.

<u>Stage 4 – Review</u>

52) Were sharing of bulk data to occur, MI5 would maintain the following ongoing obligations:

a) Undertake reviews to ensure the necessity and proportionality case for sharing continued to exist.

b) Undertake reviews of the adequacy of the arrangements governing the sharing with each recipient, including Action On, as and when necessary.

c) End current sharing with a recipient if judged necessary as a result of the above.

d) Inform the recipient of any changes to MI5's legal obligations impacting on bulk data sharing and update, as necessary, any written agreements and/or handling instructions.

SIS

53) SIS's Bulk Data Acquisition, Exploitation and Retention policy provided from 2009 onwards that:

> "17. Bulk data can be shared with other third 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 on UK National Security*."

54) SIS BPD Handling Arrangements, which came into force in November 2015 , include specific guidance to staff on the sharing of BPD with foreign partners, including:

> "7.1 The sharing of BPD is carefully managed to ensure that disclosure only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The decision to share a BPD outside SIS resists with the *senior SIS official*."

55) The guidance also states that:

> "7.3.1 *In the event that SIS deemed it was necessary and proportionate to disclose BPD to a liaison service, the same legal disclosure tests would need to be applied as when sharing with SIA partners. As part of SIS's analysis of whether disclosure is in line with its legal obligations, in the event that SIS shares BPD with a liaison service, SIS would require any such service to agree to rigorous requirements in relation to the safeguarding of that BPD. These safeguards would cover, amongst other things, access to the BPD, use (in terms of*

systems as well as purpose), and onward disclosure and will be set out on handling instructions that accompany each BPD.

7.3.2 The disclosure of BPD is carefully managed by *the relevant team* to ensure that disclosure only occurs when it is permitted under ISA 1994 and that clear necessity and proportionality cases are evidenced. Responsibility for disclosure of BPD rests with *a senior SIS official in the relevant team*."

SIS Policy on sharing BPD with foreign liaison and LEAs

[See SIS's statement of 3 March 2017, §§10-24]

56) Should SIS decide that there were an 'in principle' argument for sharing, SIS would ensure that it had a sufficient understanding of the data handling regime in the recipient organisation to enable SIS to make a reasoned judgment as to whether disclosure was necessary and proportionate in the circumstances. As part of this 'due diligence' exercise, the following are likely to be relevant considerations: the anticipated benefit to SIS; the recipient partner's requirement to obtain BPD; and the nature and extent of any handling arrangements for BPD within the recipient partner organisation (in particular in relation to access, examination, storage and onward disclosure of the BPD and/or information derived from it). In addition, SIS would seek guidance from the recipient partner as to the legal provisions applicable in that partner's jurisdiction, including whether there were any legal obligations that were likely to prevent compliance with any restrictions that SIS would want/need to place on the use of the BPD. SIS's approach to this process would be informed by its existing knowledge of and relationship with the recipient partner (including knowledge and experience of their capabilities, intent and practice).

57) Further, specifically in relation to foreign liaison and LEAs, SIS would consider any proposal to share on a case by case basis, taking into account a number of factors:

a) The nature of the partner with whom they would be sharing. This includes considering the history SIS has of sharing intelligence with that partner; their data capability and practices; and their history of compliance, either where SIS has previously shared data or where SIS has shared actionable intelligence.

b) The purpose for which it is envisaged BPD will be shared. This covers two considerations; firstly, the necessity case for SIS. At the highest level this means that there must be a requirement to share the BPD to assist SIS in meeting one of the four purposes for which

information can be shared under section 2(2) ISA. Secondly, the purpose for which SIS understand that the recipient partner wishes to obtain BPD.

Due diligence

58) The due diligence exercise would seek assurances from the proposed recipient on the relevant aspects of that partner's governance. The aim would be to establish that they have in place equivalent standards as would apply to the Agency's own staff and procedures. In practice, the specific nature of this due diligence exercise may well be tailored on a case by case basis and be subject to, for example, the particular context of the proposed arrangements or the nature of the existing relationship with that partner. The sorts of questions that SIS would seek satisfactory answers to in order to provide satisfactory assurance of equivalent standards are likely to include (but not be limited to) the following areas:

a) Relevant questions of law and policy: for example, is the partner organisation subject to provisions in law (international or domestic) that would govern their use of bulk data? Are they governed by any statutory requirements that would tie their use of bulk data to specific purposes? Are they subject to any legal obligations or policy commitments to protect the personal data or human rights of individuals?

b) Acquisition practices: for example, what factors would the partner organisation take into account before acquiring bulk data? Would necessity and proportionality be considered? Who would take part in the decision-making process and how would it be recorded?

c) Authorisation protocols: for example, what process would the partner organisation apply to authorise the retention and exploitation of BPD? What would the criteria be that would be applied to establish that it is both necessary and proportionate to retain and use data? Would legal advice be obtained?

d) Data ingestion: for example, how would BPD be stored within a partner organisation? What would the system architecture be? What other data would be stored on the system or systems? What access control mechanisms would be in place for raw and processed data? Would access control be determined by role? Would specific training be provided (including in relation to legal/policy concerns) before access is granted to a system holding bulk data? Are there categories that would be considered sensitive or privileged either by law or policy? Would ingestion of data of this type subject to additional considerations? Would there be additional protections for data of this type at the point of access?

e) Use: for example, into which tool(s) within the partner organisation would BPD be ingested? What would be the main purpose of the tool? What would a user be required to consider before searching within bulk data? Would the user be required by law to think about the necessity and proportionality and/or the direct and collateral intrusion of conducting a search? How would such considerations be recorded? Would the tool limit the nature of extent of search by a user? What safeguards would be in place to prevent misuse of BPD? Would user activity be subject to any auditing or monitoring? What would the consequences of an individual failure to comply with the law/policy on the use of BPD be? How would SIS be notified of any failure to comply and what power would they have to dictate consequences?

f) Disclosure: for example, what safeguards would be in place within the recipient organisation to ensure Action On is obtained before any action, including the passing of information to a third party, is taken on information derived from BPD? Are there legal or policy requirements to ensure that the passing of any information meets certain criteria? How would a user know that a particular piece of data requires Action On before they can use it? What would the process be for gaining Action On?

g) Retention and Review: for example, what process would be in place in the recipient organisation to review the necessity and proportionality for continuing to retain and exploit BPD? What would be the parameters for the review, and what criteria would be used to judge necessity and proportionality? What would the process be to delete data? What would the procedure be for deleting and destroying data?

h) Oversight: for example, what would be the internal and/or external oversight arrangements in place within the recipient organisation to audit the acquisition, retention and use of BPD?

59) There are a number of ways in which a due diligence exercise might be pursued and could, for example, include a visit by SIS policy and legal staff to a potential recipient to observe and discuss their systems and processes. The process would be designed to ensure that SIS would have a comprehensive written record of the way in which the recipient partner would handle BPD (covering all the matters set out at paragraph 58 above); as well as the domestic legal and compliance regime to which they are required to adhere.

60) Any such due diligence exercise would necessarily be bespoke and tailored to the partner in question and the particular circumstances of the proposed sharing arrangement. The questions set out in paragraph 58 are illustrative and neither exhaustive nor a pro forma. It is likely that any such due diligence exercise would be an iterative process. Supplementary questions may be

required for clarification and to gain an accurate and complete picture of a potential partner's governance arrangements. It is likely that SIS would seek to validate assurances given by means of 'in person' discussions with responsible officers of the partner organisation and by reference to internal policy documents, forms, codes of practice and training materials.

61) If a due diligence exercise did not result in the obtaining of satisfactory assurances, or if the veracity of assurances obtained was in doubt, the Agency would not share bulk data. In any formalising agreement or memorandum of understanding, the Agency would set out the circumstances under which the arrangement could be halted if there was concern or evidence that arrangements were not satisfactory.

Agreement to share

62) Were SIS to be satisfied with a potential recipient's data compliance following a due diligence exercise, SIS would then proceed to set out and agree with the recipient partner the detail of the agreement to share. The detail of the agreement might vary with each individual recipient depending on the circumstances and the nature of SIS's relationship with them.

Sharing of individual BPDs

63) Were SIS to agree to share BPD with a particular recipient partner, the sharing of each subsequent dataset would be considered on an individual basis. Any decision to share would be subject to a formal and recorded decision making process and would involve the input of a legal adviser where necessary. Considerations would include the necessity and proportionality case for sharing and how SIS think the recipient partner will use the data. SIS would also always consider whether the policy on Consolidated Guidance applies. The formal and recorded decision-making process would ensure that the approach to sharing outside of SIS is applied in a consistent manner.

64) SIS would ensure that dataset-specific handling instructions would accompany each BPD shared.

Monitoring compliance with assurances

65) The principal way in which compliance with the BPD handling instructions would be monitored is through the Action-On process. This is the process whereby a customer requests permission to make active use of SIS intelligence (see §31 above).

66) Any data shared with other organisations would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance, or approved through the Action-on process. Action-on is a process which is used by each of the SIAs.

67) Were SIS not to receive Action-On requests where expected, this would be investigated.

68) In addition to the Action-On process, SIS would conduct regular meetings, visits and discussions with any partners who might be in receipt of data sets. This would ensure that SIS's partners would be aware of changes to SIS's legal and compliance regime; and would enable SIS to obtain information about the changing technical, legal and compliance regimes of any partners. In that way, SIS would be able to assess on an ongoing basis whether the handling arrangements and other requirements that might apply to the sharing process remain fit for purpose.

SIS Policy on sharing BPD with industry partners

69) Although SIS can neither confirm nor deny whether it has agreed to share or in fact shares BPD with industry partners, were it to do so, it would:

a) Follow the principles and approach set out in SIS's Handling Arrangements and policy/guidance;

b) Take into account the nature of the BPD that was due to be disclosed;

c) Take into account the nature of the body to which it was considering disclosing the BPD.

BULK COMMUNICATIONS DATASETS

Cross-SIA Policy

70) The OPEN BCD Handling Arrangements which came into force in November 2015 address disclosure of BCD (at §§4.4.1 to 4.4.6):

> "**4.4 Disclosure**
> 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[3] 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:
- 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.

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.

4.4.5 Before disclosing any BCD, staff must take reasonable steps to ensure that 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 that they have received satisfactory assurances from the intended recipient organisation with respect to such arrangements.

4.4.6 These conditions must be met for all disclosure, including between the Intelligence Services and apply equally in making the decision to disclose an entire BCD, a subset of BCD, or an individual piece of data from the dataset."

Action On Process

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

71) Any data shared with other organisations would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance, or approved through the Action-on process. Action-on is a process which is used by each of the SIAs.

Commissioner oversight

72) Before 1 September 2017, the Interception of Communications Commissioner had oversight and access to all SIA material in relation to BCD compliance, including that relating to sharing. For the avoidance of doubt, that would extend to any activity of the SIA, were it to take place, relating to BCDs, including sharing with partners or giving partners remote access. See:

a) MI5 BCD Handling Arrangements of November 2015, §4.6.4(b): *"The Interception of Communications Commissioner has oversight of...(b) MI5's arrangements in respect of acquisition, storage, access...and subsequent use,* ***disclosure****, retention and destruction"* (emphasis added); and

b) GCHQ BCD Handling Arrangements of November 2015, §4.6.9: *"The Interception of Communications Commissioner is responsible for overseeing* [inter alia] ***disclosure****...of the data"*.

c) In answer to a request by the Tribunal dated 13 April 2017 about what he regards as within his remit the Interception of Communications Commissioner has confirmed, by a letter to the Tribunal dated 27 April 2017 written jointly with the Intelligence Services Commissioner, that both "use" and "disclosure" are *"taken to include sharing with other agencies or organisations, including foreign agencies."*

Since 1 September 2017 the Interception of Communications Commissioner's functions have been performed by the Investigatory Powers Commissioner.

Breaches of safeguards

73) In the event that any of the SIAs' policies and safeguards in respect of sharing BCD were breached, the relevant Agency would report any such breach to the Interception of Communications Commissioner (or now the Investigatory Powers Commissioner); investigate the breach; consider whether it remained lawful or appropriate to continue to share; if and to the

extent that any Agency staff had committed the breach in question, consideration would be given to disciplinary proceedings.

GCHQ

74) Section 4.4 of the GCHQ BCD Handling Arrangements which came into force in November 2015 addresses disclosure of BCD:

> "**4.4 Authorisation of Disclosure**
> 4.4.1 Where the results of analysing section 94 data are disclosed to partner or customer organisations, this must be done via standard intelligence reporting mechanisms, which ensure that GCHQ intelligence is released in a secure, accountable and legally compliant manner.
> 4.4.2 If disclosure of a complete section 94 dataset, or a substantial part of it, to a partner organisation is contemplated, whether at GCHQ's or the partner's initiative, the procedures below must be followed.
> ...
> 4.4.6 All requests for authorisation to disclose must provide a persuasive justification for the proposed disclosure, in terms of
> – its necessity and proportionality, and
> – the intelligence benefit or other operational benefit that is expected to accrue to GCHQ and the UK from the disclosure.
>
> 4.4.7 The Authoriser will consider:
> – the content of the dataset: the nature of any personal information it contains, its intrusiveness and sensitivity;
> – the nature and extent of the corporate risk the disclosure would entail;
> – the necessity and proportionality of the disclosure, including whether it is genuinely necessary and proportionate to disclose the whole dataset, or whether a subset will meet the need;
> – whether any caveats or restrictions should be applied; and
> – the receiving organisation's arrangements for safeguarding, using and deleting the data – GCHQ will seek additional reassurances from the receiving organisation in this regard, if the Authoriser deems it necessary."

GCHQ Policy on sharing BCD with foreign liaison/LEAs

75) GCHQ operates on the basis that operational data of any sort may only be shared if it is necessary for one of GCHQ's statutory functions, and, as far as GCHQ's intelligence gathering function is concerned, in line with one of the three purposes for which that function can be exercised. This is set out in GCHQ's Compliance Guide. All sharing is subject to compliance with all relevant legal safeguards, and there is a requirement that recipients must accord the material a level of protection equivalent to GCHQ's own safeguards. The assessment of whether a partner's

safeguards meet this standard is a matter for the Mission Policy team, in partnership with departmental legal advisors and other specialist teams as appropriate. As a matter of policy GCHQ applies the safeguards required by RIPA to all operational data even if was not obtained under RIPA powers, so this is the standard that must be met. Sharing is also subject to policy approval by an appropriately senior member of the Mission Policy team, unless an explicit delegation of approval authority has been made. Policy approval may be subject to appropriate filtering or sanitisation of the data being applied to protect sensitive material or equities.

76) The Compliance Guide makes clear that, in line with the RIPA Interception of Communications Code of Practice, particular consideration should be given in cases where confidential information (which includes, inter alia, material that is legally privileged, and confidential journalistic information) is involved. Special care must be taken to ensure that the acquisition, analysis, retention and dissemination of such material is necessary and proportionate. This covers any sharing of such data with partners. Any sharing of BCD in whole or in part is subject to formal approval by Deputy Director Mission Policy who will take into account the potential for such data to contain confidential information and ensure that this is removed from the data to the extent possible (e.g. by the removal of particular fields from datasets) and will require the application of additional or more stringent safeguards where appropriate.

77) Were GCHQ to share BCD with foreign liaison or LEAs, then it would:

a) Follow the principles and approach set out in their respective Handling Arrangements and policy/guidance.

b) Take into account the nature of the BCD that was due to be disclosed.

c) Take into account the nature/remit of the body to which they were considering disclosing the BCD.

d) Take into account the approach taken by any other SIAs who may have shared bulk data and have regard to any protocols/understanding that the other agencies may have used/followed.

e) Depending on the individual circumstance, seek assurances that the BCD in question would be handled in accordance with RIPA safeguards i.e. that it would be disclosed, copied, distributed and retained only to the minimum extent necessary for the purposes of RIPA (in the interests of National Security, for the purpose of preventing or detecting Serious Crime, or for the purpose of safeguarding the economic well-being of the UK.

78) In addition, were GCHQ to give liaison partners and/or law enforcement agencies remote access to run queries to BCD, it would apply safeguards which would put partner analysts on the same basis as GCHQ analysts. In particular, GCHQ would:

a) Require analysts to have completed all relevant training (including legalities training), be assessed as having sufficient analysis skills, and to have all necessary nationality and security clearances;

b) Require all queries to be accompanied by necessity and proportionality statements which would be subject to audit by GCHQ;

c) Require analysts to comply with GCHQ's Compliance Guide and other BCD policies and safeguards concerning access, retention and use (as set out in the Cross-SIA and GCHQ BCD Handling Arrangements);

d) Comply with the safeguards regarding the treatment of LPP and journalistic material addressed in the required training and the Compliance Guide.

GCHQ policy on sharing BCD with industry partners

79) GCHQ may share operational data with industry partners for the purpose of developing and testing new systems. Actual operational data would only be shared for such purposes if it were not possible to use standardised corpuses of non-operational data. Any sharing would be of the minimum volume of data necessary to develop or test the system. In all cases the data would be the least intrusive data that can serve the purpose. For this reason any data known or believed to contain confidential information would not be used; similar data that does not contain such material would be used instead. Wherever possible data shared with industry partners will be held on GCHQ premises, where most systems development takes place, failing that the data must be held on secure and accredited corporate premises in the UK. All sharing of data with industry is recorded on a Raw Data Release Request form which must be completed by a member of GCHQ who is sponsoring the activities of the industry partner. This form (which is used for certain other forms of data sharing which do not involve BCD) requires the sponsor to describe the purpose of the sharing and the details of the data they wish to release. If the data is to leave GCHQ premises they must specify where it is to go, and how it will be transferred. The form requires the sponsor to detail the name, organisation and job title of the individual who will take responsibility for the data on receipt, how many people at the recipient organisation will have access, for how long the

data will be retained and what will be done with it once the project is completed. These requests are assessed within the Mission Policy team and may be escalated up to the Deputy Director Mission Policy where appropriate. Mission Policy will assess each proposal to ensure that the sharing is both necessary and proportionate, and may require modification of the request if there are concerns about proportionality.

Security Service

80) Paragraphs 4.4.1 to 4.4.8 of the Security Service BCD Handling Arrangements which came into force in November 2015 address disclosure of BCD:

"**4.4 Authorisation of Disclosure**

4.4.1 The disclosure of BCD is 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 BCD, or a subset, outside MI5 may only be authorised by the Home Secretary or a Senior Official[4] in the Home Office.

4.4.2 Disclosure of individual items of communications data to persons outside MI5 can only be made if the following conditions are met:
– The objective of the disclosure falls within MI5'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;
– It is necessary to disclose the information in question in order to achieve that objective;
– The disclosure is proportionate to the objective;
– Only as much of the information will be disclosed as is necessary to achieve that objective.

4.4.3 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the communications data is 'really needed' for the purpose of discharging a statutory function of that Agency. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective – i.e. which involves less intrusion. For example, in cases where disclosure of BCD is contemplated, this could mean disclosure of individual pieces of data or of a subset of data rather than of whole BCD.

4.4.4 The disclosure of the communications data 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 MI5's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved.

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

4.4.5 Before disclosing any communications data, staff must take reasonable steps to ensure that 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 that they have received satisfactory assurances from the intended recipient organisation with respect to such arrangements.

4.4.6 These conditions must be met for all disclosure, including between the Intelligence Services. They apply equally to the disclosure of an entire BCD, a subset of the dataset, or an individual piece of data derived from the bulk communications dataset or from targeted communications data.

4.4.7 Where disclosure of **an entire BCD (or a subset)** is contemplated, (in addition to the requirement in 4.4.1 above) this is subject to prior internal authorisation procedures as well as to the requirements in 4.4.2-4.4.5 that apply to disclosure of individual pieces of data. Where these requirements are met, then (prior to submission to the Home Office/Home Secretary) the BCD is formally requested by the requesting agency from MI5 through an agreed sharing procedure using *the appropriate form*. *The data governance team* is then responsible for submitting *the appropriate form* seeking the approval of MI5's Director General. *The appropriate form* outlines the business case submitted by the requesting agency, detailing the data requested, the necessity and proportionality case for disclosure of that data and the proposed data handling arrangements.

4.4.8 If the Director General is content, a submission will be prepared for the Home Office and/or Home Secretary. Disclosure of the whole BCD (or subset thereof) is only permitted when this has been authorised by the Home Secretary or a Senior Official at the Home Office. Once authorisation has been given, arrangements will be made for the data to be disclosed to the relevant acquiring agency."

Security Service Policy on sharing BCD with foreign liaison/LEAs/industry partners

81) Were the Security Service to share BCD with foreign liaison, LEAs or industry partners, then it would only share if satisfied that:

a) Such sharing was for one of the Security Service's statutory purposes, or one of the limited additional purposes set out in s.2(2)(a) of the Security Service Act 1989.

b) It is necessary to disclose the information in question in order to achieve that objective;

c) That the disclosure would be proportionate to the objective;

d) That only as much of the information will be disclosed as is necessary to achieve that objective.

e) As set out at §4.4.5 of the Security Service BCD Handling Arrangements, the Security Service would also (a) take reasonable steps to ensure that the liaison partner has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data (including with regard to source protection and the protection of the privacy of the individuals in the BPD) and ensuring that it is securely handled, or (b) have received satisfactory assurances from the liaison partner with respect to such arrangements.

82) In the event that MI5 were considering sharing or were to share bulk data, then the approach that it would take, and the principles that it would apply, would be as described below.

83) The principles and approach that it would apply can be summarised as follows:

a) An information gathering exercise would be conducted in relation to the proposed recipient.

b) If that was satisfactory, then a sharing agreement would be prepared, if deemed necessary, to reflect the matters that MI5 considered (having regard to the information gathering exercise) needed to be covered.

c) Individual consideration of each bulk dataset to be shared would be carried out. If agreed, then any sharing of bulk datasets would be accompanied by specific handling instructions, setting out any particular requirements considered appropriate.

d) Ongoing review of the sharing relationship would be conducted.

<u>Stage 1 – information gathering</u>

84) In advance of initial sharing, and to inform the decision-making process to do so, an information gathering exercise would be undertaken to better understand the legal framework, policy and practice of the recipient. Specifically this exercise would gather information in the following areas which would inform decision making and any written agreements that were deemed appropriate:

a) <u>Law and Policy</u> – identifying the legal and policy regime that would apply in relation to bulk datasets in the recipient.

b) Acquisition of Bulk Data – identifying (if any) the process which would be applied before the recipient acquires bulk datasets and whether there is any legal and/or policy obligation to consider the necessity and proportionality of acquiring a particular dataset.

c) Authorisation – identifying the process and requirements (if any) that would be applied to authorise the retention and examination of bulk datasets.

d) Ingestion and Access – identifying how shared data would be stored, any categories of data the recipient considers sensitive (for example legal professional privilege) either by law or policy and any policy governing access to the raw dataset or intelligence derived from it.

e) Exploitation and Analysis – make reasonable enquiries regarding the use that would be made of the bulk data and the capabilities of the systems on which it would be used.

f) Disclosure – identifying any ACTION ON procedures or safeguards and the considerations taken into account when deciding to share bulk data with others.

g) Retention and Review – identifying the process and parameters by which the necessity and proportionality case for continuing to retain and exploit bulk data would be reviewed.

h) Oversight – identifying what internal and external oversight arrangements would be in place to audit the acquisition, retention and exploitation of bulk data.

85) In addition, in the event of any sharing of bulk data outside the SIA, MI5 would ensure that sharing of that data is in accordance with any wider HMG policies which MI5 is required to adhere to (for example HMG Consolidated Guidance).

Stage 2 – Sharing agreement

86) Subject to MI5 being satisfied following its information gathering exercise, a written agreement would, if considered necessary, be agreed between the recipient and MI5 in advance of any bulk data sharing. Insofar as considered appropriate, MI5 would require the recipient to apply safeguards to the handling of any shared bulk data which correspond to MI5's domestic requirements. A written agreement may detail (taking into account the results of the information gathering exercise) requirements for the following aspects of sharing:

a) How shared data will be stored, accessed and used.

b) An agreed security classification for the shared data.
c) Suitable technical and organisational measures to protect data from accidental or unauthorised disclosure or misuse.
d) A requirement that permission be sought from the disclosing partner prior to any onward disclosure from the recipient of all or part of a bulk dataset or any targeted data derived from it.
e) A requirement that permission be sought from the disclosing partner prior to any executive action being undertaken by the recipient on the basis of any shared data or targeted data derived from it.
f) A requirement that disclosure of and access to any shared data be limited to appropriately cleared personnel within the recipient who have a business justification for access to the data.
g) All staff within the recipient with access to the shared data will be made aware of the provision governing the retention and examination of the shared data made within the written agreement.
h) A requirement for the destruction of the shared data as soon as its retention is no longer deemed to be necessary or proportionate.
i) A requirement to inform the disclosing partner of any threat to life reporting obtained from examination of the shared data.
j) An assessment that the sharing of data complies with the disclosing partner's legal obligations and that the receipt of the data by the receiving partner complies with their legal obligations.

Stage 3 – Individual consideration of each bulk dataset to be shared and the terms of handling instructions to accompany each bulk dataset shared

87) In every instance where sharing of bulk data were proposed then there would need to be particular consideration of that proposed sharing, having regard to the terms of any sharing agreement in place. In each case where a bulk dataset were shared with a partner, specific handling instructions would accompany it. In addition, insofar as considered appropriate, MI5 would require the recipient to apply specific safeguards to the handling of any shared bulk data which correspond to MI5's domestic requirements appropriate to the nature of the data being shared.

Stage 4 – Review

88) Were sharing of bulk data to occur, MI5 would maintain the following ongoing obligations:

a) Undertake reviews to ensure the necessity and proportionality case for sharing continued to exist.

b) Undertake reviews of the adequacy of the arrangements governing the sharing with each recipient, including Action On, as and when necessary.

c) End current sharing with a recipient if judged necessary as a result of the above.

d) Inform the recipient of any changes to MI5's legal obligations impacting on bulk data sharing and update, as necessary, any written agreements and/or handling instructions.