IN THE INVESTIGATORY POWERS TRIBUNAL Case No. IPT/15/110/CH

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*

---

REPLACEMENT SKELETON ARGUMENT
ON BEHALF OF THE RESPONDENTS
**For hearing on 17-19 October 2017**

---

*References to the October 2017 hearing bundle are in the form [**tab number**]. References to numbered bundles used in previous hearings are in the form [**bundle number/tab number**]. References to the new authorities bundle lodged for the October 2017 hearing are in the form [**A/tab number**].*

## A. Introduction and Summary

1. This Skeleton Argument addresses the four issues that are to be determined at this hearing.[1] In the order in which they are addressed in the Claimant's skeleton, the four issues are: (1) sharing of BPD/BCD with non-SIA third parties; (2) section 94 delegation; (3) the timing of Article 8 breach and (4) ECHR proportionality.

2. The Respondents address sharing of BPD/BCD with non-SIA third parties (i.e. foreign partners, law enforcement agencies and industry partners) at **Section B** below. In summary:

   2.1. It is neither confirmed nor denied whether the Respondents share or have agreed to share BPD/BCD with foreign partners and LEAs or (in the case of SIS and MI5) with industry partners. However, were they to do so such sharing would be lawful. The Respondents set out below and in the Annex to

---

[1] The issues are set out in detail in the Appendix to the Tribunal's order dated 8 September 2017 **[tab 5(a)]**.

this skeleton the detailed safeguards and policies which would apply were they to do so.

2.2. The same safeguards apply to GCHQ's sharing of operational data, which may contain BPD/BCD, with industry partners. There has at most been extremely limited sharing of BPD/BCD with industry partners, as the 5th GCHQ witness statement explains, and it has been for the purposes of systems testing and development only.

2.3. The Claimant's criticisms of the oversight of the Investigatory Powers Commissioner and, before 1 September 2017, of the oversight of the Intelligence Services Commissioner and the Interception of Communications Commissioner are misplaced. Sharing of BPD/BCD, were it to occur, is and was within their remit. The Claimant's challenge to the efficacy of these regimes founded on apparent shortcomings in oversight by the Commissioners in relation to GCHQ sharing of BPD/BCD with industry partners is misconceived - the scale of the sharing in question was so small that any failings in respect of it cannot possibly lead to the conclusion that oversight generally was inadequate.

2.4. The Respondents' policy regarding whether or not recipients of BPD/BCD would be required to give *"equivalent"* protection to that given by the Respondents themselves is also clear. Insofar as considered appropriate the Respondents would seek to ensure that the recipients afforded the information an equivalent level of protection to their own safeguards.

2.5. The Claimant's further assertion that the sharing of BCD outside the EU or with LEAs is incompatible with EU law can only be determined in the light of the outcome of the reference that the Tribunal has decided to make to the CJEU. For the avoidance of doubt, the Respondents will submit that such matters fall outside the scope of EU law in any event.

2.6. In the circumstances, the Respondents' safeguards that apply to the sharing of BPD/BCD with non-SIA third parties, were it to occur, are *"in accordance with law"* and consistent with the requirements of the ECHR.

2.7. The question of whether the Respondents do in fact comply (and, historically, have in fact complied) with those safeguards is the subject of CLOSED evidence.[2] In order to determine Issue 4 on List of Issues appended to the 8 September 2017 order, the Tribunal will therefore need to conduct some form of CLOSED process.

---

2 Other than GCHQ sharing with industry partners, which is essentially an OPEN issue

3. At **Section C** below, the Respondents address the Claimant's argument that GCHQ's s.94 directions unlawfully delegate powers to GCHQ officials. The reality is that the GCHQ official in question has no more than a formal power to do what the Foreign Secretary has directed. The official has no discretion as to how to exercise that power, nor has any such official ever purported to do so. In practice the official has simply put into effect what the Foreign Secretary has directed, and has done so immediately following the making of the direction.

4. **Section D** responds to the Claimant's contention that section 94 directions made prior to avowal should be quashed, thus rendering the operation of the regime post-avowal unlawful notwithstanding the Tribunal's core conclusion in its October 2016 judgment that the BCD regime was lawful in the period following avowal. Specifically, the Respondents contend that it would be inappropriate to quash the s.94 directions, in circumstances, *inter alia*, where (i) the Tribunal found that the regime was contrary to Article 8 ECHR on grounds of foreseeability and insufficient oversight, but not lack of *vires* of the directions themselves, and (ii) the consequence of a quashing order would be to render the post-avowal operation of the s.94 regime unlawful, given the ongoing effect of directions made before avowal.

5. Finally, at **Section E** below, the Respondents deal with the proportionality arguments as now advanced by the Claimant, insofar as it is possible to do so in OPEN. In summary, the Respondents' s.94 BCD and BPD activities are proportionate and have been throughout the relevant period:

   5.1. In the field of national security a wide margin of appreciation is accorded to the Government in assessing the pressing social need and choosing the means for achieving the legitimate aim of protecting national security (see *Liberty/Privacy*, §§33-39).

   5.2. The United Kingdom faces serious national security threats, including from international terrorism (where the threat level is SEVERE) and from hostile states. Developments in technology, particularly the increasing use of encryption, make capabilities such as BCD and BPD much more important to the SIAs.

   5.3. The usefulness of BCD obtained under s.94 directions is clear. It provides more comprehensive coverage than is possible by means of interception. For example, it enables GCHQ to *"tip off"* the Security Service when a subject of interest arrives in the UK. Security Service investigations are made more sophisticated and timely as a result of having a BCD database rather than having to rely solely on individual CD requests made to CSPs.

   5.4. The BCD capability also leads to a significant *reduction* of the intrusion into privacy of individuals of no intelligence interest. Analysis of BCD, and of

patterns of communication and potential subjects of interest, enables identification of specific individuals without first having to carry out more intrusive investigations into a wide range of individuals.

5.5. BPD is also a highly important capability for each of the SIAs. It has been used e.g. to identify a suspected Al-Qaida operative using fragmentary information to reduce possible candidates from 27,000 to one. The speed of analysis as a result of the use of electronic BPDs is of particular importance.

5.6. The importance of BPDs to the SIAs has been accepted in emphatic terms by David Anderson QC, the Independent Reviewer of Terrorism Legislation, in his August 2016 *Report of the Bulk Powers Review*. He noted, inter alia, their *"great utility to the SIAs"* and found that case studies which he examined *"provided unequivocal evidence of their value"*. He found that the work of MI5 and SIS *"would be substantially less efficient without the use of BPDs"* and also accepted the utility of BPDs to GCHQ *"to enrich information obtained through other means."* In the *"vital"* areas of pattern analysis and anomaly detection, which can provide information about a threat in the absence of any other intelligence, *"no practicable alternative to the use of BPDs exists."* He concluded that the operational case for BPD is *"evident"*.

5.7. The use of BPD also significantly reduces the needs for more intrusive techniques to be used. The identification of targets from a wider pool by means of searching BPDs avoids the need to investigate that wider pool in a more intrusive manner. The electronic nature of the searches also means that the data of subjects which is searched but does not produce a *"hit"* will not be viewed by the human operator of the system but only viewed electronically.

5.8. For these reasons, the use of BPDs, and BCD obtained under s.94 directions is and has at all times been proportionate. The Respondents have filed CLOSED evidence that is relevant to this issue; it will be necessary for the Tribunal to consider that evidence before finally determining this issue.

## B. Sharing of BPD/BCD

6. In its October 2016 judgment, and in its subsequent order of 31 October 2016, the Tribunal held that the BPD and BCD regimes were lawful under Article 8 ECHR from the dates of their respective avowal, and unlawful prior to those dates. However, the Tribunal wished to give *"further consideration...to the provisions for safeguards and limitations in the event of transfer by the SIAs to other bodies, such as their foreign partners and UK Law Enforcement Agencies."* **[tab 2(a)/§95]** The remaining issue therefore concerns transfer of BPD and BCD by the SIAs to non-SIA third parties, in

particular *"UK law enforcement agencies, commercial companies or foreign liaison partners"* (Claimant's skeleton, §2(b)).

7. This broad topic covers numbered issues 3, 4 and 5 on the List of Issues appended to the 8 September 2017 order **[tab 5(a)]**.

Preliminary question – the meaning of 'Bulk Personal Dataset'

8. The Claimant argues (skeleton, §5) that a dataset of raw sigint data is itself a BPD, as defined in the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015 ("the 2015 Direction") **[A/tab 7]**. This is a novel suggestion, which the Claimant has raised at a time when this litigation has been proceeding on a different basis for several years. The Respondents do not accept this suggestion – see generally §§13-21 of the Amended 5th witness statement of the GCHQ witness dated 7.7.17 **[tab 4(k)]**.

9. The 2015 Direction defined *"bulk personal dataset"* as follows:

> *"any collection of data...which comprises personal data as defined by section 1(1) of the Data Protection Act 1998...relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest [and] is held, or acquired for the purposes of holding, on one or more analytical systems within the Security and Intelligence Agencies."*

10. Had a dataset of raw sigint data been intended to fall within this definition surprising results would have followed. When the 2015 Direction came into force oversight over interception, and intercept data, was the responsibility of the Interception of Communications Commissioner. The 2015 Direction, which put on a statutory basis the Intelligence Service Commissioner's existing oversight over BPDs, would, if the Claimant is right, either have transferred oversight over raw sigint data from the Interception of Communications Commissioner to the Intelligence Services Commissioner, or would have created joint oversight. Neither such inconvenient result was intended. The 2015 Direction cannot sensibly have been meant to carve out raw sigint data from the Interception of Communications Commissioner's interception-specific role and expertise. Nor can it have been intended to make *both* Commissioners responsible for oversight over the same datasets, given the duplication of resources this would entail. Either such intention would also no doubt have been stated in express words, but was not.

11. This is reinforced by the OPEN BPD Handling Arrangements **[2/B/183-193]**, §10.1 of which recognises the intention that the Intelligence Services Commissioner's oversight should only extend to data that would not otherwise fall within the statutory remit of the Interception of Communications Commissioner. Furthermore, the Investigatory Powers Act 2016 maintains the distinction between bulk data

acquired through interception (which falls within Part 6) and bulk personal datasets (which fall within Part 7). See s.201(1) of that Act.

12. Of course, for understandable reasons, when a dataset of raw sigint data is processed in such a way that it becomes a Bulk Personal Dataset (and is intended to be placed on an agency's analytical systems with other BPDs for ongoing use/access by investigators), then that dataset becomes subject to the BPD Handling Arrangements (though still under the oversight of the Interception of Communications Commissioner): see §§17-18 of the Amended 5th GCHQ statement **[tab 4(k)]**. However, that is a separate question from whether raw sigint data falls within the 2015 Direction, as the Claimant contends, or whether raw sigint data is automatically a BPD. For reasons given above, it is not.

13. For all of these reasons, the Claimant's contention that a dataset of raw sigint data is a BPD, and that the evidence concerning the transfer of BPDs is incomplete (skeleton, §5(e)), is incorrect.

The law

14. As the Tribunal held at §37 of its judgment in *Liberty/Privacy* **[A/tab 12]**, in order for an interference to be "*in accordance with the law*":

> "*i) there must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action.*
>
> *ii) the nature of the rules must be clear and the ambit of them must be in the public domain so far as possible, an "adequate indication" given (Malone v UK [1985] 7 EHRR 14 at paragraph 67), so that the existence of interference with privacy may in general terms be foreseeable...*"

See also *Bykov v. Russia*[3], at §78, quoted at §37 of *Liberty/Privacy*.

15. As the Tribunal also noted in *Liberty/Privacy*, in the field of national security much less is required to be put into the public domain and therefore the degree of foreseeability must be reduced, because otherwise the whole purpose of the steps taken to protect national security would be put at risk (see §§38-40 and §137). See also in that respect, *Malone v UK*[4] (at §§67-68m), *Leander v Sweden*[5] at §51 and *Esbester v UK*[6], quoted at §§38-39 of *Liberty/Privacy*. Thus, as held by the Tribunal in the *British Irish Rights Watch* case[7] (a decision which was expressly affirmed in the *Liberty/Privacy* judgment at §87): "*foreseeability is only expected to a degree that is*

3 Appl. no. 4378/02, 21 January 2009 **[A/tab 27]**.
4 (1984) 7 EHRR 14 **[A/tab 19]**.
5 [1987] 9 EHRR 433 **[A/tab 20]**.
6 [1994] 18 EHRR CD 72 **[A/tab 21]**.
7 IPT decision of 9 December 2004 **[A/tab 9]**.

*reasonable in the circumstances, and the circumstances here are those of national security..."* (§38)

16. Thus, the national security context is highly relevant to any assessment of what is reasonable in terms of the clarity and precision of the law in question and the extent to which the safeguards against abuse must be accessible to the public (see §§119-120 of the *Liberty/Privacy* judgment).

17. As to the procedures and safeguards which are applied, two points are to be noted.

17.1. It is not necessary for the detailed procedures and conditions which are observed to be incorporated in rules of substantive law. That was made clear at §68 of *Malone* and §78 of *Bykov*; and was reiterated by the Tribunal at §§118-122 of *Liberty/Privacy*. Hence the reliance on the Code in *Kennedy v United Kingdom*[8] at §156 and its anticipated approval in *Liberty v United Kingdom*[9] at §68 (see §118 of *Liberty/Privacy* and also *Silver v United Kingdom*[10]).

17.2. It is permissible for the Tribunal to consider rules, requirements or arrangements which are "below the waterline" i.e. which are not publicly accessible. In *Liberty/Privacy* the Tribunal concluded that it is *"not necessary that the precise details of all of the safeguards should be published, or contained in legislation, delegated or otherwise"* (§122), in order to satisfy the "in accordance with the law" requirement; and that the Tribunal could permissibly consider the *"below the waterline"* rules, requirements or arrangements when assessing the ECHR compatibility of the regime (see §§50, 55, 118, 120 and 139 of *Liberty/Privacy*). At §129 of *Liberty/Privacy* the Tribunal stated:

> *"Particularly in the field of national security, undisclosed administrative arrangements, which by definition can be changed by the Executive without reference to Parliament, can be taken into account, provided that what is disclosed indicates the scope of the discretion and the manner of its exercise...This is particularly so where:*
>
> *i. The Code...itself refers to a number of arrangements not contained in the Code...*
>
> *ii. There is a system of oversight, which the ECHR has approved, which ensures that such arrangements are kept under constant review."*

17.3. Those conclusions were reached in the context of the s.8(4) RIPA interception regime. They are equally applicable to the s.94 and BPD regimes to which published Handling Arrangements and *"below the waterline"* arrangements apply and where there is similar oversight by the Investigatory Powers

---

8 [2011] 52 EHRR 4 **[A/tab 29]**.
9 [2009] 48 EHRR **[A/tab 25]**.
10 [1983] 5 EHRR 347 **[A/tab 18]**.

Commissioner (and previously by the Intelligence Services Commissioner and the Interception of Communications Commissioner).

18. In the context of interception, the ECtHR has developed a set of minimum safeguards in order to avoid abuses of power. These are referred to as 'the *Weber* requirements'. At §95 of *Weber*[11], the ECtHR stated:

> *"In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed."* (numbered items added for convenience, see §33 of *Liberty/Privacy*)

(And see also *Valenzuela Contreras v Spain*[12] at §59)

19. However it is important to recognise what underpins the *Weber* requirements, as highlighted at §119 of the *Liberty/Privacy* judgment. In particular, §106 of *Weber* states as follows:

> *"The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life,* ***it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security*** *(see, inter alia, Klass and Others, cited above, p. 23, § 49; Leander, cited above, p. 25, § 59; and Malone, cited above, pp. 36-37, § 81).* ***Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse*** *(see Klass and Others, cited above, pp. 23-24, §§ 49-50; Leander, cited above, p. 25, § 60; Camenzind v. Switzerland, judgment of 16 December 1997, Reports 1997-VIII, pp. 2893-94, § 45; and Lambert, cited above, p. 2240, § 31).* ***This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law*** *(see Klass and Others, cited above, pp. 23-24, § 50)."* (emphasis added)

---

11 (2008) 46 EHRR SE5 [**A/tab 23**].

12 (1999) 28 EHRR [**A/tab 22**].

20. The Tribunal in *Liberty/Privacy* placed considerable reliance on oversight mechanisms in reaching their conclusion that the intelligence sharing regime and the s.8(4) RIPA regime were Article 8 compliant. In particular:

20.1. The role of the Commissioner and "*his clearly independent and fully implemented powers of oversight and supervision*" have been long recognised by the ECtHR, as is evident from *Kennedy* **[A/tab 29]** at §§57-74, 166, 168-169 (see *Liberty/Privacy* at §§91-92). This is a very important general safeguard against abuse. In *Liberty/Privacy* the Tribunal relied, in particular, on his duty to keep under review the adequacy of the arrangements required by statute and by the Code, together with his duty to make a report to the Prime Minister if at any time it appeared to him that the arrangements were inadequate.

20.2. The advantages of the Tribunal as an oversight mechanism were emphasised at §§45-46 of *Liberty/Privacy*, including the "*very distinct advantages*" over both the Commissioner and the ISC for the reasons given at §46 of the judgment.

20.3. In addition the ISC was described as "*robustly independent and now fortified by the provisions of the JSA*" (see §121 of *Liberty/Privacy*) and therefore constituted another important plank in the oversight arrangements.

20.4. Consequently there is a need to look at all the circumstances of the case and the central question under Art. 8(2) is whether there are: "*...adequate arrangements in place to ensure compliance with the statutory framework and the Convention and to give the individual adequate protection against arbitrary interference, which are sufficiently accessible, bearing in mind the requirements of national security and that they are subject to oversight.*" (see §125 of the *Liberty/Privacy* judgment)

Sharing of BPD/BCD with foreign partners

21. There are considerable limits on the Respondents' ability to address in OPEN the matters which are relevant to the restrictions that might be placed in relation to sharing of BPD or BCD with foreign partners if such sharing were to occur. CLOSED evidence has been filed, of which some has been disclosed into OPEN. See:

21.1. GCHQ's Amended OPEN statement of 6 March 2017 **[tab 4(g)]**;

21.2. Security Service's OPEN Statement of 10 February 2017 **[tab 4(c)]**, together with a further OPEN statement dated 10 April 2017 **[tab 4(h)]**; and

21.3. SIS's Amended OPEN Statement of 3 March 2017 **[tab 4(f)]**.

22. The SIAs neither confirm nor deny whether they have agreed to share or in fact have shared or do share BPD or BCD with foreign liaison: see GCHQ's statement of 6.3.17, §9; SyS's statement of 10.2.17, §§8-10; SIS's statement of 3.3.17, §§9 and 11.

23. The Claimant contends that GCHQ has now avowed that it shares BPD with the 5-Eyes partners (Claimant's skeleton, §25) (although, for avoidance of doubt, no such argument is made in respect of BCD, or SIS and MI5).

24. This contention is incorrect as a consideration of the documents relied on by the Claimant (skeleton, §§24-25) reveals:

24.1. The term *"Sigint and non-Sigint data"*, which is quoted by the Claimant (skeleton, §24), is very broad. It does not purport to specify which 5-Eyes partners in fact provide Sigint data or non-Sigint data to GCHQ, or indeed which types of Sigint data or non-Sigint data are provided. It should not be read as admitting to all possible combinations of partner type and information type. It is a statement in a Code of Conduct for non-GCHQ staff (from other SIAs or government departments) of the need to obtain permission from a partner in the event that a 5-Eyes partner does share certain types of data with GCHQ. Unsurprisingly, given the nature of the document, it does not spell out in detail the precise nature and scope of any provision of data by particular 5-Eyes partners with GCHQ.

24.2. The policy goes no further than referring to Sigint and non-Sigint data being provided by 5-Eyes partners to GCHQ. Nothing is said about provision of Sigint and/or non-Sigint data in the other direction – i.e. by GCHQ to 5-Eyes partners. The document does not therefore amount to any sort of avowal of any sharing undertaken by GCHQ with 5-Eyes partners.

24.3. Furthermore, even if (contrary to the above) the policy was to be read as indicating sharing of Sigint and/or non-Sigint data with 5-Eyes partners, it contains no reference whatsoever to the provision of BPD by GCHQ.

25. The Claimant relies (skeleton, §25) on two other documents to make its argument that (contrary to its clear terms) the GCHQ policy document avows GCHQ's sharing of BPD with 5-Eyes partners:

25.1. The first is the UKUSA Agreement. This document is over 60 years old. There is plainly a limit to the practical application of such a document to GCHQ's relationship with partners in 2017. In any event, although the Claimant notes the references in Article 4 and Appendix C, §3 that *"each party will continue to make available to the other continuously, currently, and without request, all raw traffic."* they do not note that it was subject to exceptions (see §§4(b) and 5(c) of the Agreement), as Appendix C, §3, read in its entirety, makes clear. For the

avoidance of doubt, it has never been the case – either at the time the UKUSA Agreement was signed, or subsequently - that all raw traffic, or indeed all other material, is made available to the NSA or 5-Eyes partners by the UK. Finally, there is no reference whatsoever to BPD in the UKUSA Agreement. In the circumstances, nothing material to the Claimant's argument that GCHQ has avowed that it shares BPD with foreign partners is contained in the UKUSA Agreement.

25.2. The second document is David Anderson QC's Bulk Powers Review of August 2016 [**A/tab 33**]. The Claimant notes footnote 119, which states *"Some BPDs are obtained by interception..."* It appears to be suggested by the Claimant that it therefore follows that such intercepted BPDs are shared with the 5-Eyes foreign partners. However, the argument contains a logical leap. As explained above, there has been and is no avowal that all intercepted material is shared with the 5-Eyes foreign partners.

26. For these reasons, the Claimant's submission that *"it has now been confirmed by official sources that there is sharing of data held in BPDs with the Five Eyes foreign partners"* (Claimant's skeleton, §25) is simply incorrect. The Respondents continue neither to confirm nor deny whether they have agreed to share or in fact have shared or do share BPD or BCD with either foreign liaison or LEA.

27. As to the matters set out at §§26-27 of the Claimant's skeleton argument in reliance on alleged "Snowden documents", the Respondents do not contend that the Claimant is not entitled to rely on these documents. But no admissions are made either as to the authenticity of the documents, or as to the veracity of their contents. If the Tribunal thinks it necessary, further submissions can be made on these matters in CLOSED.

28. The Respondents do, however, assert that it would be lawful to share with foreign partners and LEAs, and set out in the Annex to this skeleton the safeguards and policies which would apply were they to do so.

29. In summary, in relation to **BPD**:

29.1. Any sharing of BPD must be authorised in advance by a senior individual within the sharing Agency: see Joint SIA BPD Policy of February 2015 (Annex, §28)

29.2. The relevant necessity and proportionality tests for onward disclosure under the SSA or ISA would have to be met: Joint SIA, BPD Policy of February 2015 (Annex, §28) Cross-SIA OPEN BPD Handling Arrangements, §§5.2, 6.1 (Annex, §29), as would the statutory safeguards under the SSA, ISA, CTA, HRA, DPA and OSA (Annex, §§3-27).

29.3. Guidance on the meaning of "necessity" and "proportionality" is given: Cross-SIA OPEN BPD Handling Arrangements, §§6.2, 6.3 (Annex, §29)

29.4. 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. (Annex, §31); see Joint SIA BPD Policy (Annex, §28).

29.5. Before disclosing BPD, as part of the consideration of proportionality, staff must *"consider whether other, less intrusive methods can be used to achieve the desired outcome"* Cross-SIA OPEN BPD Handling Arrangements, §5.2, and also §6.3 (Annex A, §29).

29.6. Sensitive BPDs, or fields within a BPD containing sensitive data, must be protected if it is not judged to be necessary or proportionate to share them: Joint SIA BPD Policy (Annex, §28)

29.7. Before disclosing any BPD, staff must take reasonable steps to ensure the intended recipient *"has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data"* and also ensuring that it is "securely handled" or have received satisfactory assurances from the intended recipient with respect to such arrangements Cross-SIA OPEN BPD Handling Arrangements, §6.4 (Annex, §29).

29.8. Detailed policies exist in relation to sharing BPD: see Annex, §§37-40, 45-52 and 56-68. These would include:

a. Carrying out information gathering exercises, including into:
   i. The nature of the proposed recipient;
   ii. The legal and policy regime that would apply in relation to BPDs in the recipient;
   iii. The nature and extent of any process for handling BPDs within the recipient partner organisation, in particular in relation to acquisition, authorisation, ingestion/access, exploitation/analysis, disclosure, retention/review and oversight of BPD/information derived from BPD;
b. Entering into a written agreement, where necessary, with the recipient where necessary/appropriate detailing requirements for the sharing of BPD;
c. Individual consideration of each BPD to be shared and the terms of handling instructions to accompany each BPD shared.

d. Monitoring/reviewing the necessity/proportionality of continued sharing and the adequacy of the recipients arrangements for sharing;
e. Ending sharing with a recipient if judged necessary;
f. Informing the recipient of any changes to their legal obligations impacting on bulk data sharing and updating, as necessary, any written agreement and/or handling instructions.

29.9. Insofar as considered appropriate the Respondents would seek to ensure that the recipients afforded the information an equivalent level of protection to the Respondents' own safeguards. This would be effected in appropriate cases by the procedures set out above and in the Respondents' witness statements (GCHQ statement of 6.3.17, §§6-11; MI5 statement of 10.4.17, §§4-10; SIS statement of 3.3.17, §§9-24), including requiring the proposed recipient to apply safeguards to the handling of any shared BPD which corresponded to the Respondents' own domestic requirements.

29.10. Disclosure of the whole or a subset of a BPD is subject to internal authorisation procedures. An application must be made to a senior manager designated for the purpose. This must describe the BPD intended to be disclosed, set out the operational and legal justification for the proposed disclosure, and whether any caveats or restrictions should be applied to the proposed disclosure. This is so the senior manager can then consider the relevant factor with operational, legal and policy advice taken as appropriate. See Cross-SIA OPEN BPD Handling Arrangements, §6.7 (Annex, §29).

29.11. In difficult cases, the relevant Intelligence Service may seek guidance or a decision from the Secretary of State: Cross-SIA OPEN BPD Handling Arrangements, §6.7 (Annex, §29).

29.12. *"Wider legal, political and operational risks would also have to be considered, as appropriate"*: Joint SIA BPD Policy (Annex, §28)

29.13. The disclosure of a BPD (as in the case of its acquisition or retention) is subject to scrutiny in each Intelligence Service by an internal Review Panel, whose functions include *"to ensure that...any disclosure is properly justified"*: Cross-SIA OPEN BPD Handling Arrangements, §8.1 (Annex, §30).

30. The Agency-specific Handling Arrangements, and relevant authorisation forms, reflect the requirements of the overarching Cross-SIA OPEN BPD Handling Arrangements. See:

30.1. The GCHQ BPD Handling Arrangements and its Bulk Personal Data Acquisition Retention (BPDAR): Annex, §§35 and 36.

30.2. The Security Service's BPD Guidance of March 2015, its BPD Handling Arrangements of November 2015 and its Form for Sharing: Annex, §§42-44.

30.3. SIS's Bulk Data Acquisition, Exploitation and Retention policy from 2009 onwards and the SIS BPD Handling Arrangements of November 2015: Annex, §§53-55.

31. As for **BCD**:

31.1. Disclosure of an entire BCD or a subset of a BCD outside the Intelligence Service may only be authorised by a Senior Official, equivalent to a member of the Senior Civil Service, or the Secretary of State: see the Cross-SIA BCD Handling Arrangements, §4.4.1 (Annex, §70).

31.2. The relevant necessity and proportionality tests for onward disclosure under the SSA or ISA would have to be met: Cross-SIA BCD Handling Arrangements, §§4.4.1-4.4.2 (Annex, §70) as would the statutory safeguards under the SSA, ISA, CTA, HRA, DPA and OSA (Annex, §§3-27).

31.3. Guidance on the meaning of *"necessity"* and *"proportionality"* is given: Cross-SIA OPEN BCD Handling Arrangements, §§4.4.3-4.4.4 (Annex, §70)

31.4. 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. (Annex, §71).

31.5. Before disclosing BCD, as part of the consideration of proportionality, staff must *"consider whether there is a reasonable alternative that will still meet the proposed objective – i.e. which involves less intrusion."* Cross-SIA OPEN BCD Handling Arrangements, §4.4.4 (Annex, §70).

31.6. Before disclosing any BCD, staff must take reasonable steps to ensure the intended recipient *"has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data"* and also ensuring that it is *"securely handled"* or have received satisfactory assurances from the intended recipient with respect to such arrangements Cross-SIA OPEN BCD Handling Arrangements, §4.4.5 (Annex, §70).

31.7. Again, as with BPD, there are policy requirements in place (see Annex, §§75-78, 81-88) requiring:

a. Carrying out information gathering exercises, including into:
   i. The nature of the proposed recipient;

ii. The legal and policy regime that would apply in relation to BCDs in the recipient;

iii. The nature and extent of any process for handling BCDs within the recipient partner organisation, in particular in relation to acquisition, authorisation, ingestion/access, exploitation/analysis, disclosure, retention/review and oversight of BCD/information derived from BCD;

b. Entering into a written agreement, where necessary, with the recipient where necessary/appropriate detailing requirements for the sharing of BCD;

c. Individual consideration of each BCD to be shared and the terms of handling instructions to accompany each CPD shared.

d. Monitoring/reviewing the necessity/proportionality of continued sharing and the adequacy of the recipients arrangements for sharing;

e. Ending sharing with a recipient if judged necessary;

f. Informing the recipient of any changes to their legal obligations impacting on bulk data sharing and updating, as necessary, any written agreement and/or handling instructions.

31.8. Again, insofar as considered appropriate GCHQ and MI5 would seek to ensure that the recipients afforded the information an equivalent level of protection to their own safeguards. This would be effected in appropriate cases by the procedures set out above and in the Respondents' witness statements (GCHQ statement of 6.3.17, §§6-11; MI5 statement of 10.4.17, §§4-10), including requiring the proposed recipient to apply safeguards to the handling of any shared BCD which corresponded to GCHQ/MI5's own domestic requirements.

32. Again, the Agency-specific Handling Arrangements reflect the requirements of the overarching Cross-SIA OPEN BCD Handling Arrangements. See:

32.1. The GCHQ BCD Handling Arrangements of November 2015: Annex, §74;

32.2. The Security Service's BCD Handling Arrangements of November 2015: Annex, §80.

33. In light of the above, the Claimant's submission that *"[t]here are no published arrangements governing the safeguards to be applied when considering sharing of data with foreign intelligence services or other UK law enforcement agencies"* (Claimant's skeleton, §38) is quite obviously wrong.

34. Further, the Claimant is wrong to suggest that the Respondents' position in respect of *"equivalence"* is unclear (Claimant's skeleton, §§38-40): see §29.9 and §31.8 above. More generally on this issue:

34.1. The whole question of obtaining 'equivalent' safeguards when (hypothetically) sharing data with foreign partners is one that the Tribunal should approach with care. In most cases, the simple transposition of domestic safeguards will be neither appropriate nor necessary.

34.2. It is self-evident that if data is passed to organisations that are differently configured to UK agencies and that operate under different legal orders, the detail of the safeguards needed are likely to be different to those set out in domestic arrangements. That is why the agencies' policies emphasise the need for an information-gathering exercise when sharing is first considered.

34.3. Moreover, the need for any particular 'equivalent' safeguards is likely to vary according to the nature of any data shared.

34.4. Proportionality considerations will also apply. If, for example, there was an urgent need to share data in order to respond to a threat to life, different 'equivalence' considerations would apply than in other cases.

34.5. It is these and other similar considerations that inform the Respondents' general position, as set out above, that *"Insofar as considered appropriate the Respondents would seek to ensure that the recipients afforded the information an equivalent level of protection to the Respondents' own safeguards."*

35. Furthermore, the Respondents submit that the published arrangements set out above, and in detail in Annex A, satisfy the requirement in *Weber* at §106 that *"there exist adequate and effective guarantees against abuse"* and in *Liberty/Privacy* at §125 that there are *"...adequate arrangements in place to ensure compliance with the statutory framework and the Convention and to give the individual adequate protection against arbitrary interference, which are sufficiently accessible, bearing in mind the requirements of national security and that they are subject to oversight."*

36. The Claimant also asserts that there is *"little, if any"* Commissioner oversight over sharing of BCD/BPD (Claimant's skeleton, §18, §43). This is denied. The Investigatory Powers Commissioner (and, before 1 September 2017, the Intelligence Services Commissioner and Interception of Communications Commissioner) has oversight and access to all GCHQ, Security Service and SIS material in relation to BPD/BCD governance (as applicable), including that relating to sharing, were it to occur. The Tribunal has upheld the adequacy of the Commissioners' oversight throughout (at least) the post-avowal period.[13] Furthermore:

36.1. The Intelligence Services Commissioner Additional Review Functions (Bulk Personal Datasets) Direction 2015, pursuant to which 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*

13 Since 2010 in the case of BPD and since July 2015 in the case of BCD (October 2016 judgment, §§80-82) [tab 2(a)/§§80-82].

*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) (see Annex, §33). The Investigatory Powers Commissioner has oversight over BPD

36.2. The Interception of Communications Commissioner had oversight over all aspects of disclosure of BCD (see Annex, §72).

36.3. In answer to a request by the Tribunal dated 13 April 2017 about what they regarded as within their remit both Commissioners confirmed, by a joint OPEN letter dated 27 April 2017, that both "use" and "disclosure" are *"taken to include sharing with other agencies or organisations, including foreign agencies"* **[tab 6(b)]**.

37. The Claimant's criticisms regarding Commissioner oversight of GCHQ sharing of BPD/BCD with industry partners are addressed below.

38. The Respondents therefore contend that their policies that would relate to the sharing of BPD and BCD with foreign partners are lawful and consistent with Article 8 ECHR. Related issues of EU law are addressed at §61 below.

39. Issue 4 on the List of Issues appended to the 8 September 2017 order calls for an examination by the Tribunal of what (if any) sharing of BPD and/or BCD with foreign partners (and also with industry partners and domestic law enforcement agencies) has in fact taken place, and whether any such sharing complied with relevant safeguards. CLOSED evidence relating to these factual matters has been served. In order to determine Issue 4, the Tribunal will need to adopt some form of CLOSED process.

Sharing with law enforcement partners

40. As with foreign sharing, the Respondents neither confirm nor deny in OPEN whether they share BPD or BCD with law enforcement agencies.[14] Detailed CLOSED evidence has been filed.

41. What can be said in OPEN is that, were such sharing to take place, then the processes and safeguards set out above would apply.

42. It is also possible to address in OPEN, at the level of principle, the Claimant's argument that for the Respondents to share BPD or BCD with law enforcement agencies would amount to an unlawful circumvention of the safeguards in the TA

[14] For statements of this position, see the references at paragraph 22 above

1984, RIPA and DRIPA. Prior to the July 2016 hearing, the Tribunal formulated assumed facts against which to test this point, as follows:

> *"It is to be assumed for the purposes of this hearing:*
>
> *(a) that a Programme exists by which GCHQ discloses information to domestic law enforcement agencies ("LEAs"); and*
>
> *(b) that this disclosure might take place either*
>
> *(i) by GCHQ permitting the LEAs to access and search data that it holds, including communications data obtained pursuant to section 94 directions; or*
>
> *(ii) by GCHQ providing the LEAs with information derived from the data that it holds, including communications data obtained pursuant to section 94 directions."*

43. As stated above, the Respondents neither confirm nor deny whether a 'Programme' of the type referred to exists, or whether in general terms the type of data sharing referred to in the assumed facts takes place. The Respondents do, however, submit that it would be lawful for GCHQ to provide data, obtained by means of s.94 directions to other government law enforcement agencies ('LEAs'), on the basis that those other LEAs required the data for the purposes of combating serious crime.

44. Obtaining CD produced by CSPs pursuant to directions issued under s.94 falls within GCHQ's statutory functions set out at s.3(1)(a) of the Intelligence Services Act 1994 ('ISA') **[A/tab 2]**:

> ***"3 The Government Communications Headquarters.***
>
> *(1)There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be –*
>
> *(a) 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;... "*

45. The purpose for which GCHQ obtains s.94 data is in the interests of national security, which is one of the statutory purposes as listed at s.3(2) of ISA:

> *"(2) The functions referred to in subsection (1)(a) above shall be exercisable only –*
>
> *(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."*

46. Section 19(2) of the Counter-Terrorism Act 2008 ('CTA') **[A/tab 5]** then expressly provides:

> *"(2) Information obtained by any of the intelligence services[15] 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."*

Given that GCHQ may exercise its statutory functions in support of the prevention or detection of serious crime (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.

47. Section 19(5) of the CTA provides that:

> *"(5) Information obtained by GCHQ for the purposes of any of its 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."*

Since the purpose for which GCHQ may exercise its statutory functions include supporting the prevention or detection of serious crime, GCHQ is entitled to disclose s.94 data to LEAs for that purpose.

48. Finally, s.4(2) of ISA **[A/tab 2]** 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..."*

49. It follows that any disclosure of such information must satisfy the constraints imposed in ss.3-4 of the ISA, as read with s.19(5) of the CTA **[A/tab 5]**. Additionally any such disclosure must comply with the necessity and proportionality requirements imposed b and s.6(1) of the HRA. Thus specific statutory limits are imposed on the information that GCHQ can disclose.

---

15 Section 21(1) of CTA provides that *"In sections 19 and 20 "the intelligence services" means the Security Service, the Secret Intelligence Service and GCHQ."* **[A/tab 5]**

Sharing with industry partners

50. GCHQ shares operational data with industry partners for the purpose of developing its systems. Its safeguards are explained at §41 of the Annex. The Security Service and SIS neither confirm nor deny whether they share bulk data with industry partners. Were they to do so, the policies which apply to disclosure of BPD/BCD generally would apply.

51. The factual context of GCHQ's sharing of BPD and BCD with industry partners is explained in detail in the Amended Fifth Statement of the GCHQ Witness dated 7 July 2017 **[tab 4(k)]**, and also in the Response (dated 26 July 2017) to the Request for Further Information that was made in relation to the Fifth Statement **[tab 3(k)]**.

52. The critical factual starting point is that GCHQ sharing of BPD and BCD with industry partners by remote access and by transfer since 2010 has been extremely limited. Specifically (references are to paragraphs in the Amended GCHQ Fifth Statement):

52.1. A single database containing non-sensitive BPD has been accessed remotely by a small number of individuals (fewer than 20) (§29(b)) and no BPD at all has been transferred to industry partners (§33(a)).

52.2. No BCD at all has been accessed remotely (§29(a)), and the only possible example of the transfer of BCD are some samples of operational data in 2010-11 that may have contained BCD (§33(b)).

53. Moreover:

53.1. In the case of remote access (see criticisms at §§14-22 of the Claimant's skeleton), there are substantial safeguards to prevent non-compliance or abuse by industry partners - see §§26-28 and 24 of the Amended 5th GCHQ statement **[tab 4(k)]**.

53.2. In the case of transfer of data (see criticisms at §§10-13 of the Claimant's skeleton), any such transfer is only made to industry partners' systems which have been accredited and where it can be accessed only by vetted staff (GCHQ Amended Fifth Statement, §31). Such transfers may only be made by completion of a Raw Data Release Request Form which must be submitted by a GCHQ sponsor and approved by the GCHQ policy team (*ibid.*, §32; see also Annex, §41).

54. The Claimant's principal criticism relating to GCHQ sharing with industry partners is of an alleged lack of oversight by the Commissioners (skeleton, §§18-22).

55. The criticisms made by the Claimant have to be set in the context of the extremely limited nature of the transfer of, or provision of remote access to, BPD/BCD by

GCHQ to industry partners. As set out above, in the case of BCD it is possible, and no more, that operational data transferred to industry partners in 2010-11 may have contained section 94 data. There have been no other instances. In the case of BPD, one database containing non-sensitive BPD has been accessed remotely by a small number of industry partners' (vetted) employees. This was for the purpose of systems testing alone. (*ibid.*, §29(b)).

56. It is submitted that even if the Commissioners were not aware of the possibility of sharing of BPD/BCD in such *de minimis* amounts (although they had been briefed on other aspects of GCHQ's work with industry partners), that is not sufficient to render an entire regime unlawful or non-compliant with Article 8 ECHR.

57. It is a matter of common sense that no body of Commissioners, regardless of their resourcing or expertise, could ever exercise practical and continuing oversight over every relevant activity undertaken by the organisation under supervision. It follows that where it is said that the Commissioners have failed to investigate or to have proper regard to a particular practice, the seriousness of the failing (and indeed the question of whether there was a failing at all) must be judged, amongst other things, against the scale of the activity in question and also the risks involved. Where, as is the true factual position regarding GCHQ's provision of remote access and transferring BPD/BCD to industry partners, the practice (a) took place on an extremely limited basis; and (b) was supported by practical safeguards such as the accreditation of the computer systems and the vetting of the personnel involved, then any 'failing' that may be said to have taken place is at the lowest end of the scale.

58. Furthermore, it is important to recall in this context that the Commissioners represent only one limb of the system of judicial oversight in this field. This Tribunal is another limb of that system - and one that the Strasbourg Court in *Kennedy* [**A/29**] clearly considered to be at least as important as the Commissioners. The very fact that the Tribunal is investigating this issue in the present case demonstrates the efficacy of its oversight role.

59. Finally, any shortcoming in this regard is now historic, as the Investigatory Powers Commissioner has confirmed that, having been advised of the issues raised by this case *"the IPC immediately ordered that an inspection of those UKIC agencies that may share datasets should be undertaken. I can confirm that these inspections have now occurred."* (Answer to Question 4, IPC's letter of 19 September 2017) [**tab 6(h)**].

60. In summary, the Claimants' submissions in this regard go too far. There is, and has been, substantially adequate Commissioner oversight over sharing/disclosure of BPD/BCD, and that would clearly extend to any such sharing/disclosure with third parties. It is a further very important general safeguard against abuse.

EU law

61. The Claimant repeats (at skeleton §§44-50) its submission that following the CJEU's decisions in *Watson* and *Opinion 1/15*, BCD may neither be transferred out of the EU nor shared with LEAs for serious crime investigations that do not raise any national security issue.

61.1. As to the transfer of BCD out of the EU, the Tribunal has already decided to make a reference to the CJEU on this issue: see §§65-68 of the Tribunal's judgment of 8 September 2017 **[tab 2(b)]**.

61.2. As to the sharing of BCD obtained under a section 94 direction with LEAs for the purposes of the investigation of serious crime, and as set out at §40 above, it is neither confirmed nor denied in OPEN that any such sharing takes place. Insofar as any question of the lawfulness of such sharing were to arise for decision, it could only be determined following the outcome of the Tribunal's order for reference to the CJEU: it begs the question as to whether any such sharing falls within the scope of EU law. The Respondents' position is that:

61.2.1. Any such sharing would fall outside the scope of the Treaty and of the e-Privacy Directive. On any basis, as the Tribunal indicated at §48 of its judgment of 8 September 2017, it is difficult to see how the ambit of the e-Privacy Directive applies *after* acquisition by the SIAs.

61.2.2. Moreover, the sharing of BCD (whether in the form of the provision of access to data held by the SIAs or in the form of the provision of information derived from BCD held by the SIAs) would not amount to an activity of any provider of electronic communications services, and so (even if falling within the scope of the Treaty) would be excluded from the scope of the e-Privacy Directive: Article 1(3) excludes the activities of the State in areas of criminal law from the Directive's scope.

61.2.3. In any event, the Claimant's references to the CJEU's decision in Opinion 1/15 take the matter no further. There are already clear and precise rules as to the purposes for which such BCD may be used. See §§43-49 above on the specific statutory authorisation for GCHQ to use s.94 data for the purpose of the prevention or detection of serious crime, and its disclosure for that purpose. Accordingly, the Claimant's suggestion at §50 of its skeleton argument that there is *"no express statutory authorisation for the sharing"* of BCD is incorrect.

## C. Section 94 delegation

62. The Claimant argues that the section 94 directions used by GCHQ unlawfully delegate powers to GCHQ officials, and frustrate the legislative purpose behind

section 94 (skeleton, §§51-65). This is a highly technical point. It is devoid of any substantive merit.

63. The Respondents have served a detailed witness statement addressing this issue - the 4th GCHQ witness statement dated 16 June 2017 [**tab 4(i)**]. That statement provides the relevant factual context, and demonstrates why the Claimant's arguments on this point are misconceived. By way of summary the Respondents submit as follows.

64. **First**, the only power that is given to the GCHQ official is a power to trigger the effect of a decision that has already been taken by the Foreign Secretary. Under both the old direction (Exhibit GCHQ 9) and the new direction (Exhibit GCHQ 10) the GCHQ official had power only to *"request"* data from the CSP which the Foreign Secretary had already directed the CSP to provide. No discretion is conferred by either form of direction. In truth, there is no more than a formal power on the part of the GCHQ official which enables the direction - and subsequent changes to the precise data to be provided under the direction, as authorised by the Foreign Secretary - to have effect.

65. **Second**, as a matter of fact, the *"triggering"* has always taken place immediately following the making of the direction:

> *"These initial requests, and subsequent changes, were always made immediately following the making of the direction by the Foreign Secretary, or his authorising a variation in the data to be provided under a direction."* (§9 of the 4th GCHQ statement)

66. This reinforces the point already made: there has never been any question of the GCHQ official exercising any discretion. He has simply acted to put into effect - immediately - the decision of the Secretary of State.

67. **Third**, the decision as to the selection of data which the CSP was directed to provide has also been that of the Secretary of State, not the GCHQ official. Although not set out in the old form of direction (Exhibit 9), they were *"routinely set out in the submission to the Foreign Secretary that invited the making of the direction, and then communicated to the CSP in correspondence after the direction was made."* (4th GCHQ statement, §12(a)). Any changes had to be approved by the Foreign Secretary (*ibid.*, §12(c)-(d)). That the selection of data was and is a decision of the Foreign Secretary is plain from the new direction (Exhibit GCHQ 10), but was no less true when the old direction was used.

68. There is therefore no question of any *"circumvention"* or frustration of the statutory powers or purposes as the Claimant contends (skeleton, §§58-59) nor has the Respondents' submission in this litigation that s.94 directions are made by a Secretary of State been misleading (contrary to Claimant's skeleton, §62). There is no impact on the compliance of the section 94 BCD Regime with EU law, Article 8 ECHR or domestic law.

## D. Timing of Article 8 breach

69. The Claimant contends (skeleton, §§66-71) that the effect of the Tribunal's October 2016 judgment was that the earliest date from which obtaining BCD pursuant to section 94 directions was lawful was 14 October 2016 – i.e. nearly a year later than the date of avowal (4 November 2015).

70. The importance of this argument is, as the Claimant notes (skeleton, §71), the remedy that should flow from the unlawfulness identified by the Tribunal.

71. The Respondents submit that it is necessary to keep carefully in mind the different issues – and the different type of issues – that the Tribunal was considering when it reached its conclusions on s.94 BCD in the October 2016 judgment [**tab 2(a)**].

72. Issue 1 was in the following terms: *"Section 94 TA under domestic law: Is it lawful as a matter of domestic law to use s.94 TA to obtain BCD?"* (see §16 of the October 2016 judgment). The question was therefore a pure *vires* point. Was there in fact power under s.94 to make the directions requiring the production of BCD? If the Tribunal had found in favour of the Claimant on that point, the remedy would no doubt have been to quash the section 94 directions. However, the Tribunal did not do so – it rejected the Claimant's *vires* arguments.

73. Issue 2 was of a different nature:

> *"Is the s.94 TA regime in accordance with the law? This issue is to be considered in three time periods. First, prior to the avowal of the use of s.94 to obtain BCD [4th November 2015]. Secondly, from avowal to the date of hearing. Thirdly, as at the date of hearing."*

74. Rather than focusing on the section 94 directions, this issue addressed *"the section 94 **regime**"* (emphasis added). That is, it encompassed the making of the directions, the production of the BCD, the holding, use and destruction of BCD, the publication of handling arrangements, and so on. The question was whether that *entire* regime complied with Article 8. Furthermore, the agreed terms of the order required the Tribunal to consider Article 8 compliance at different times – pre-avowal; post-avowal; and at the date of trial.

75. The Tribunal considered the BCD regime in depth, and concluded that it did not comply with Article 8 prior to avowal, for reasons solely relating to the foreseeability of the regime and the sufficiency of oversight – but that it did comply following avowal: see §§70-71, 84(ii) and 101 of the October judgment.

76. The Tribunal's conclusion to this effect was encapsulated in paragraph 2 of its Order of 31 October 2016, which stated that *"The Respondents' [BCD] 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."*

77. The nature of the conclusions that the Tribunal reached in its October 2016 judgment are highly significant to the question of remedy that the Claimant raises now. The appropriate relief is of course a matter of discretion: s.67(7) RIPA gives the Tribunal power to *"make any such award of compensation* ***or other order as they think fit"*** (emphasis added). The Claimant appears to suggest that any s.94 directions made prior to avowal should be quashed (skeleton, §66). The Respondents submit that that would be an entirely inappropriate order, given that:

77.1. The Tribunal has rejected the direct *vires* challenge to the section 94 directions;

77.2. The grounds on which the Tribunal found the s.94 regime to be in breach of Article 8 did not relate to the directions themselves, but to wider issues – the lack of publicity and the efficacy of the oversight arrangements.

77.3. An order quashing directions made prior to avowal would have the effect of rendering unlawful the operation of the regime during the post-avowal period. This is of course precisely why the Claimant contends for this remedy: see skeleton, §66, final sentence. However, it is also a powerful reason why the remedy should not be granted, since its effect would run precisely contrary to the substance of the Tribunal's finding, which is that the s.94 regime operated lawfully from the time of avowal onwards.

77.4. Put another way, the relief that the Claimant now seeks is inconsistent with paragraph 2 of the Tribunal's Order of 31 October 2016.

78. For these reasons, the most suitable remedy for the Tribunal to grant in light of its reasoned findings is simply a declaration that the s.94 regime did not comply with Article 8 prior to avowal but did so afterwards. An order to that effect has already been made. Nothing further is either required or appropriate.

## E. Proportionality

79. It is only ECHR proportionality that is in play at this stage; the question of proportionality under EU law principles has been deferred pending the reference.

80. There are considerable limits on the Respondents' ability to address in OPEN the matters which are relevant to an assessment of the proportionality of their activities. However the following brief OPEN submissions are made at this stage.

81. As is made clear eg. in *Leander v Sweden* **[A/20]**, in the field of national security the Government has a wide margin of appreciation in assessing the pressing social need

and in choosing the means for achieving the legitimate aim of protecting national security (see §§58-59 and see also the Tribunal's conclusions in Liberty/Privacy [**A/12**] at §§33-39).

82. As explained in detail in the MI5 witness statement [**Core/B/2**] of 8 July 2016 at §§6-33 the threat from international terrorism throughout the relevant period, from the July 2005 London transport attacks onwards, has been significant. The current threat level is SEVERE; indeed, on two occasions in 2017 the threat level has been raised to CRITICAL. Serious threats are also posed by hostile states and serious and organised crime (§§18-21). Developments in technology, in particular the increasing use of encryption (§§22-33), make other capabilities, such as BCD and BPD, much more important to the SIAs.

83. There is a clear value to BCD obtained by s.94 directions:

83.1. For GCHQ: *"The specific value of communications data obtained from CSPs under section 94 direction is that it provides more comprehensive coverage than is possible by means of interception under section 8(4) of RIPA"* (GCHQ statement [**Core/B/2**], §115). This provides *"a higher level of assurance that it can identify e.g. patterns of communications than it could be means of interception alone."* (ibid.). Examples of the usefulness of BCD to GCHQ's activities are set out at §§120 of the GCHQ statement (e.g. enabling GCHQ to "tip off" the Security Service when a subject of interest arrives in the UK), and §§155-162 (e.g. where an analysis of BCD assisted in identifying a terrorist group and understanding the links between members in a way which *"would not have been possible...at speed by relying on requests for targeted communications data"* (§156); see also §159 for an example involving the disruption of a bomb plot against multiple passenger aircraft).

83.2. The MI5 statement [**Core/B/2**] also emphasises the need for a database of BCD: *"in complex and fast-moving investigations, having access to a database of BCD would enable MI5 to carry out more sophisticated and timely analysis, by joining the dots in a manner that would not be possible through individual CD requests made to CSPs."* (MI5 statement, §110). See also ibid., §§152-3, and the emphasis on the speed of BCD techniques compared with other techniques.

84. It is also important to note that the BCD capability in fact leads to a significant reduction of the intrusion into privacy of individuals of no intelligence interest: GCHQ statement, §116; MI5 statement, §153. Analysis of BCD, and the resultant identification of patterns of communication and potential subjects of interest, enables specific individuals to be identified *without* having first to carry out more intrusive investigations into a wider range of individuals.

85. BPD is a highly important capability for each of the SIAs. Examples of its usefulness are given at:

85.1. MI5 witness statement of 8 July 2016 **[Core/B/2]**, §38 (suspected Al-Qaida operative identified from fragmentary information; searching a BPD, and matching with two others reduced possible candidates from 27,000 to one), §108;

85.2. GCHQ statement of 8 July 2016 **[Core/B/2]**, §§16-18, §§106-114;

85.3. SIS statement of 8 July 2016 **[Core/B/2]**, §8, §21 (identification of an individual planning to travel to Syria out of hundreds of possible candidates).

The speed of analysis as a result of the use of electronic BPDs is of particular importance: MI5, §§39-40; §107; GCHQ statement, §111.

86. The BPD capability also significantly reduces the need for *more* intrusive techniques to be used. The MI5 statement gives an example of how searches of BPD enabled the identity of a suspect for whom a general description had been provided, but no name, to one strong match. More intrusive methods could then be justified *in respect of that individual alone*. Without BPD MI5 would have had to investigate a wider range of individuals in a more intrusive manner: MI5 statement, §108; see also GCHQ statement, §§107, 114; SIS statement, §17, §21.

87. Furthermore, the *electronic* nature of searches of BPD reduces the intrusion into privacy (*"any data which is searched but which does not produce a "hit" will not be viewed by the human operator of the system, but only searched electronically."*: MI5 statement, §48). In reality *"the personal data of the vast majority of persons on a BPD will never, in fact, be seen read or considered by MI5 because it will never feature as a search result."* (ibid., §105). See also the GCHQ Statement, §19 (*"Using BPD also enables the Intelligence Services to use their resources more proportionately because it helps them exclude potential suspects from more intrusive investigations."* (§19)), and the example at §107.

88. The August 2016 *Report of the Bulk Powers Review* by David Anderson QC, the Independent Reviewer of Terrorism Legislation **[A/33]**, emphatically accepted the importance of BPDs to the SIAs:

*"8.33 I have no hesitation in concluding that BPDs are of **great utility** to the SIAs. The case studies that I examined provided **unequivocal evidence of their value**. Their principal utility lies in the identification and development of targets, although the use of BPDs may also enable swift action to be taken to counter a threat.*

*8.34 BPDs are already used elsewhere, in the private as well as the public sector, with increasing sophistication. Their utility to the SIAs has been acknowledged by successive IsComms and by the ISC…As I concluded in AQOT 8.106: "It may legitimately be asked, if*

*activity of a particular kind, is widespread in the private sector, why it should not also be permitted (subject to proper supervision) to public authorities".*

*8.35 BPDs are used by the SIAs for many purposes: for example, to identify potential terrorists and potential agents, to prevent imminent travel, and to enable the SIAs to prioritise work. It will often be possible, in a given instance, to identify an alternative technique that could have been used. However many such alternatives would be slower, less comprehensive or more intrusive.* ***The value of accurate information, obtained at speed, is considerable.*** *I accept the claims of MI5 and MI6 that their work would be* ***substantially less efficient without the use of BPDs and GCHQ's claim that it finds BPDs useful to enrich information obtained through other means.***

*8.36 In some areas, particularly pattern analysis and anomaly detection,* ***no practicable alternative to the use of BPDs exists.*** *These areas of work are vital, since they can provide information about a threat in the absence of any other intelligence seed. The case studies included a cogent example of the value of pattern analysis (A11/2).*

*8.37 The use to which bulk data can be put is in the course of rapid evolution. MI5 recognised in July 2015 that the development of new technologies and data types, including machine learning and predictive analysis, offered "additional promise" in this field. Future decision-makers authorising and approving the use of BPDs will have to be aware of these technological advances, and the effect that they have both on the availability of alternatives and on the extent of intrusion involved in the use of BPDs."* (emphasis added)

89. The conclusion of the report was unequivocal: *"The operational case for [BPDs] is evident"* (§9.14(d)).

90. Further detail on these points is given in the Third Witness Statement of the GCHQ Witness dated 2 March 2017 **[tab 4(e)]**. This statement was considered in detail at the EU law hearings earlier this year and the Tribunal is familiar with its contents.

91. At §§73-75 of its skeleton argument, the Claimant refers to a single paragraph from the *Bulk Powers Review*, containing David Anderson QC's observations on 'reducing the privacy footprint', and seeks to build on those observations an argument that the entire BPD/BCD regimes are disproportionate. This argument is wholly misconceived. The Respondents make the following brief points in response.

    91.1. The suggestion at §75 of the Claimant's skeleton that *"none of the witnesses called by the Agencies has made any attempt to address the proportionality of the use of BPD and BCD or how privacy consequences of the collection and use of such datasets can be minimised"* is plainly wrong. That is the very purpose of the various Handling Arrangements and other safeguards that are discussed at length in the Respondents' evidence.

    91.2. The fact that proposals have been made to equip the Commissioners with greater expertise and/or resources does not mean that the existing regime is

inadequate from an Article 8 perspective, far less that the entire regime is disproportionate. Similar, highly detailed questions to those that are posed at §74 of the Claimant's skeleton might have been asked of the oversight regime at issue in *Kennedy*, which the Strasbourg court regarded as discharging a valuable function for article 8 purposes.

92. The Respondents contend that both the s.94 BCD regime and the BPD regime are proportionate under Article 8 ECHR and have been throughout each of the relevant periods. CLOSED evidence relating to this issue has been filed; it will be necessary for the Tribunal to consider this evidence before finally determining this issue.

**JAMES EADIE QC**

**ANDREW O'CONNOR QC**

**ROBERT PALMER**

**RICHARD O'BRIEN**

**6 October 2017**

**Re-served with cross-references on 12 October 2017**

**Annex: 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") [**A/tab 2**];

   b) the Counter-Terrorism Act 2008 ("the CTA") [**A/tab 5**];

   c) the Human Rights Act 1998 ("the HRA") [**A/tab 3**];

   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 **[tab 2(a)]**. 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

b) to take appropriate technical and organisational measures to guard against unauthorised or

[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.

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 [**SIS statement, 3.3.17 at tab 4(f)**]:

> **"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 **[2/B/183-193]** 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;" **[2/B/188]**

"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." **[2/B/190-191]**

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." **[2/B/191-192]**

**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 [**3/110-119**] addresses disclosure of BPD at section 9 [**3/115-116**]:

"**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 [**3/41-57**], 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."* [**3/50**]; and

b) Requires identification of whether the BPD contains any sensitive personal data, and if so what kind [**3/43**].

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 [**1/40**]:

> "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 **[1/101-113]** address disclosure outside the SIA in section 6 **[1/109-110]**:

"**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" [**1/89-93**]. 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 [**1/90**]

b) Access restrictions: the *"arrangements agreed to ensure material is handled securely and what access control will be applied"* must be stated [**1/90**]

c) Agreed caveats in relation to the handling of the material must also be set out [**1/90**]

d) The "Business Justification & Privacy Assessment" requires the statutory purpose and a necessity and proportionality assessment to be set out [**1/90-91**], and approved by a senior MI5 official.

e) The technical feasibility of disclosure must be approved by the relevant technical team [**1/92**]

f) Legal approval for disclosure must also be given by a legal adviser [**1/92**].

g) Final approval must also be given by DSIRO or designated person [**1/92-93**]

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