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 in the week commencing 5 June 2017

---

*References to the authorities in the bundles lodged with the Tribunal are in the form: [**A/vol/tab**] (the authorities bundles served for the July 2016 hearing), [**SA/vol/tab**] (the Supplementary Authorities bundle served for the 8-10 March 2017 hearing) or [**2SA/tab**] (the Second Supplementary Authorities bundle served for the 5-9 June 2017 hearing). References to the hearing bundles are in the form [**bundle/tab**] (the July 2016 hearing bundles), [**Supp/tab**] (the Supplemental bundle lodged for the 8-10 March 2017 hearing) or [**2Supp/tab**] (the Second Supplemental bundle lodged for the 5 May 2017 hearing).*

A. Introduction and Summary

1. This Skeleton Argument replaces and supersedes: the Respondents' Outline Response to the Claimant's EU law submissions dated 17 February 2017; the Skeleton Argument of the Respondents dated 2 March 2017; the Annex to the Respondents' Skeleton Argument dated 3 May 2017; and the Respondents' Outline Response to the Tribunal's Questions, dated 10 May 2017. It addresses the three issues that fall for determination at this hearing, namely: (1) the impact of EU law; (2) sharing of BPD/BCD with non-SIA third parties; and (3) proportionality.

2. The Claimant's EU law arguments are addressed at **Sections B to E** below. The Claimant's argument on the EU law issues amounts to the assertion that the CJEU's judgment in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* and *Watson & ors* ("***Watson***") [**SA/1/17**] can be applied directly to both the directions made under s.94 of

the Telecommunications Act 1984 to a CSP, and to the obtaining of BPDs. In each case, the Claimant contends that the effect of *Watson* is:

2.1. that the relevant regime engages EU law pursuant to Directive 2002/58/EC ("***the e-Privacy Directive***") [**SA/1/5**] in the case of s.94 directions and Directive 95/46/EC ("***the Data Protection Directive***") [**SA/1/4**] in the case of BPDs.

2.2. that bulk retention of BCD and BPDs is unlawful under EU law; and

2.3. that the use of such BCD and BPDs lack safeguards which are mandatory under EU law, namely:

2.3.1. a requirement for prior independent authorisation for access;

2.3.2. procedures for notification of use of the data;

2.3.3. adequate controls on how they are shared; and

2.3.4. a prohibition on the transfer outside of the EU.

3. It is submitted first that s.94 directions and the BPD regime do not engage EU law: see **Section B** below. In summary:

3.1. The European Union may only act, and the EU Charter only applies, within the limits of competences conferred upon it by the Member States in the Treaties. Competences not conferred upon the Union in the Treaties remain with the Member States. Matters of Member States' national security are not conferred on the EU. On the contrary, they are positively identified as being the sole responsibility of Member States in Article 4(2) TEU [**SA/1/1**]. Further, such matters do not constitute a derogation from EU law and are not to be interpreted restrictively. Since primary EU law cannot be altered by any secondary EU measures, the scope of the e-Privacy Directive and the Data Protection Directive does not and cannot extend to activities of Member States in support of national security. Each of those Directives excludes those activities from their scope (as they must).

3.2. Accordingly, insofar as relevant to the issues in this litigation, the activities of the SIAs, including in relation to the obtaining of information/data from third parties (including CSPs) under the SSA 1989, the ISA 1994 and the TA 1984, are outside the ambit of EU law. The mere fact that information/data is – necessarily – acquired by the SIAs from other individuals (including providers of electronic communications services) is not sufficient to engage EU law: the acquisition of personal data for analysis by the SIAs is the paradigm example of national security activity, and core to the SIAs' ability to function.

3.3. Further and in any event, even in the context of the fight against serious crime by law enforcement agencies (distinct from the field of national security), the use of BCD

acquired under a s.94 direction and of BPDs falls outside the scope of the Directives. The Claimant is incorrect to suggest that *Watson* is authority for the proposition that any retention of or access to communications data or BPDs falls within the scope of EU law. The Swedish laws at issue in *Tele 2 Sverige* and DRIPA were both analysed by the CJEU as imposing a requirement on electronic communications service providers to retain and provide access to communications data. Even in the field of criminal law, the CJEU made clear that "*activities of the State"* do not fall with the scope of the Directives, and are to be distinguished from the activities of providers of electronic communications services or any other individuals. The CJEU did not address the acquisition and use of BCD and BPD by the State.

4. Further, neither the effect of a s.94 direction nor of the BPD regime is to require providers or any other individual to retain any data. The Claimant's central premise that a s.94 direction is materially identical to a DRIPA retention notice, and that BPD is no different, is incorrect. See **Section C** below.

5. Alternatively, even were EU law engaged, with the result that a proportionality analysis was required to be undertaken in respect of the justification for the use of s.94 directions and BPDs against the interference with rights under Article 7 and 8 of the Charter, the safeguards identified in the context of *Watson* are not to be read across and applied here. On the (incorrect) hypothesis that EU law, and the requirements of the Directives in particular, are engaged:

   5.1. In the context of national security, the effect of Article 4(2) TEU is that a Member State has the broadest possible margin of discretion to judge what is necessary and proportionate in the interests of national security. The use of s.94 directions and BPDs in the work of the SIAs is judged to be necessary and proportionate to national security.

   5.2. The safeguards identified in *Watson* were judged by the CJEU to be necessary and appropriate in the case of a requirement on service providers to retain and disclose communications data for the purposes of the targeted investigation, detection and prosecution of serious crime, to which the court's judgment in *Watson* is directed. But it does not follow that those particular safeguards must, or can properly, be likewise applied in the context of any use of bulk data by the SIAs (or indeed other state authorities, including law enforcement agencies). To the contrary, they cannot sensibly be applied in the context of the acquisition or use of BCD under a s.94 direction or of BPDs. Such safeguards are neither adaptable nor appropriate to such circumstances. To do so would significantly undermine the ability of the SIAs to protect the public by protecting the UK's national security.

6. In those circumstances, any proportionality analysis that was required to be undertaken would yield the result that the existing regime is lawful. Alternative safeguards are in place which are suitable and proportionate to the circumstances of the nature of the data in question and of the use to which the data are put. As has already been held by this

Tribunal, such safeguards are in accordance with those required by the ECHR; and, if that is so, it is impossible to see why it should be appropriate or permissible to require more, especially when the effect would be to introduce serious risks to national security. See **Section D** below.

7. The Claimant is accordingly wrong to argue that *Watson* can be applied to the BCD or BPD regimes rather than to the requirements under Swedish law and DRIPA on electronic communications services providers to retain and/or provide access to data for the purposes of the investigation, detection and prosecution of serious crime.

   7.1. Alternatively, if and to the extent that the judgment in *Watson* suggests that the CJEU purported to make any findings in relation to the retention of and/or access to databases acquired and held by the SIA for the purposes of national security, any such ambiguity as to scope of the judgment should be resolved by reading the judgment consistently with the scope of the jurisdiction conferred on the EU, and therefore on the CJEU, by the Treaties.

   7.2. In the further alternative, if the Tribunal considers that the judgment in *Watson* is incapable of being read consistently within the limits of EU competence set at the European Treaty level, the Tribunal should make a reference to the CJEU pursuant to Article 267 TFEU [**2SA/1**] to clarify the CJEU's position. If the CJEU were to confirm beyond doubt that it intended to apply the EU Charter to the retention of and/or access to data for the purposes of national security, notwithstanding the non-conferral of competence on the EU in relation to matters of national security, the question would then arise as to the proper course of action for a domestic court faced with a judgment of the CJEU that exceeds its jurisdiction. That would be a question of domestic law as to the proper interpretation of the European Communities Act 1972: see *Pham* [2015] 1 WLR 1591 at §§75ff., *per* Lord Mance. See **Section E** below**.**

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

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

   8.2. The same safeguards apply to GCHQ's sharing of operational data, which may contain BPD/BCD, with industry partners.

8.3. The Claimant's criticisms of the oversight of the Intelligence Services Commissioner's and Interception of Communications Commissioner's oversight are misplaced. Sharing of BPD/BCD, were it to occur, would plainly be within their remit, as they have expressly confirmed.

8.4. 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.

8.5. In the circumstances, the Respondents' policy for sharing of BPD/BCD with non-SIA third parties, were it to occur, is *"in accordance with law"* and lawful both as a matter of the ECHR and of EU law.

9. Finally, at **Section G** 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:

9.1. 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).

9.2. 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 and increasing difficulty of interception, make capabilities such as BCD and BPD much more important to the SIAs.

9.3. 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.

9.4. 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.

9.5. 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.

9.6. 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"*.

9.7. 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.

9.8. For these reasons, the use of BPDs and BCD obtained under s.94 directions is and has at all times been proportionate.

B. The s.94 and BPD regimes fall outside the scope of the Directives

(i) National security falls outside the scope of EU law and the Directives

10. Article 4(1) and (2) TEU [**SA/1/1**] provide as follows (underlining added):

> "*1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the Member States.*
>
> *2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."*

11. Article 5(1) and (2) TEU [**SA/1/1**] further provide:

> "*1. The limits of Union competences are governed by the principle of conferral. ...*
>
> *2. Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States."*

12. Notably, in the International Law Decision of 18-19 February 2016 [**SA/2/31**], it was confirmed that

> "*Article 4(2) of the Treaty on European Union confirms that national security remains the sole responsibility of each Member State. This does not constitute a derogation from Union law and should therefore not be interpreted restrictively. In exercising their powers, the Union institutions will fully respect the national security responsibility of the Member States*."[1]

13. The effect of Article 4(2) was more recently explained in Case C-51/15 *Remondis* [**SA/1/16**]. That case concerned the issue of whether the definition of "*public contracts*" in the EU directive on public procurement extended to an agreement between two regional authorities to form a common special-purpose association with separate legal personality. The CJEU answered it by reference to Article 4(2) TEU, adopting the view of Advocate-General Mengozzi that such matters fell outside the scope of EU law altogether. It is apparent that:

    13.1 The matters covered by Article 4(2) are solely matters for each Member State and do not fall under EU law. The fact that the Union must respect "*essential State functions*" (including the division of responsibility as between national, regional and local government, and, in the present case, national security) is consistent with the principle of conferral of powers laid down in Articles 5(1) and (2) TEU, no provision having conferred on the Union the power to intervene in such matters: see the Opinion of AG Mengozzi at §§38-39.

    13.2 As acts of secondary legislation such as a directive must be in conformity with primary law (i.e. the Treaties), they cannot be interpreted as permitting interference in the matters which benefit from the protection conferred by Article 4(2) TEU. Such matters remain outside the scope of EU law and, more specifically, EU rules set out in a directive: see the Opinion of AG Mengozzi at §§41-42, as endorsed by the CJEU in its Judgment at §§40-41.

[1] On 18-19 February 2016, the Heads of State or Government of the 28 Member States of the European Union, meeting within the European Council, made a Decision concerning a new settlement for the United Kingdom within the European Union. At section C.5 of the Decision, the Heads of State and Government stated that The Decision did not formally come into force given that the United Kingdom did not vote to remain a member of the European Union in the referendum. However, in accordance with Article 31 of the Vienna Convention on the Law of the Treaties, it remains an interpretative decision agreed by all parties to the EU Treaties.

14. National security is quintessentially such a matter, as emphasised not only by the second sentence of Article 4(2) TEU but also the third sentence. This has always been the position: the Lisbon Treaty's introduction of Article 4(2) simply articulated that competence for national security has not, and never has been in the past, conferred on the Union.

15. Thus, when Article 16(2) TFEU [**SA/1/2**] provides for the EU legislature to make rules on the protection of personal data, it does so in terms that confine the power only to those activities of Member States which fall within the scope of EU law (underlining added):

> "*The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States <u>when carrying out activities which fall within the scope of Union law</u>, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*"

16. Likewise, in Title V of Part Three of the TFEU (relating to the Area of Freedom, Security and Justice) [**SA/1/2**], it is confirmed that responsibility for national security remains with Member States, and is not conferred upon the EU. See:

    16.1 Article 72 TFEU provides: "*This Title shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security*"; and

    16.2 Article 73 TFEU provides: "*It shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security.*"

    16.3 Similarly, Article 276 TFEU makes clear that "*in exercising its powers regarding the provisions of Chapters 4 and 5 of Title V of Part Three relating to the area of freedom, security and justice, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.*"

17. While they pre-date the Lisbon Treaty, consistently with the position set out in Article 4(2) TEU and Article 16(2) TFEU, both the Data Protection Directive and the e-Privacy Directive specifically exclude national security from their scope.

    17.1 Article 3(2) of the Data Protection Directive [**SA/1/4**] provides that it "*shall not apply to the processing of personal data in the course of an activity which*

falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law."[2]

17.2 Article 1(3) of the e-Privacy Directive [**SA/1/5**] provides that it "*shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law*."[3]

18. Likewise, in the General Data Protection Regulation (Regulation (EU) 2016/679 [**SA/1/7**], which will repeal and replace the Data Protection Directive with effect from 25 May 2018, Recital (16) makes clear:

> "*This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security.*"

19. It is plain from those provisions that the EU legislature intended to confine the scope of each of the Directives to those activities falling outside the various identified areas. That was inevitable in the case of national security and essential State functions, given that competence in such matters has not been conferred upon the EU (or the European Community before it) at all, as Article 4(2) TEU and Article 16(2) TFEU make clear.

(ii) Application to s.94 directions and BPDs

20. Once it is acknowledged that Article 4(2) TEU excludes activities concerning national security from the scope of EU law, the only issue is what activities may be properly categorised as falling within that concept. In considering that issue it is to be noted that Article 4(2) is not a derogation, and is thus not to be interpreted narrowly.

21. The acquisition and use of personal data (including communications data) for the purpose of identifying and disrupting national security threats is a core national security activity. Indeed, it is a paradigm activity of the SIAs, who rely on the acquisition of personal data to provide the raw material of intelligence. It falls squarely within the heart of Article 4(2) TEU.

22. In Joined Cases C-317/04 and C-318/04 *Parliament v Council* [2006] ECR I‑4721 [**SA/1/9**], the CJEU held at §59 that a Commission Decision that adequate arrangements had been made for the protection of bulk PNR data (collected for airlines'

[2] See also Recital (13) of the Data Protection Directive.
[3] See also Recital (11) of the e-Privacy Directive.

commercial purposes) transferred by airlines to the United States authorities fell outside the scope of the Data Protection Directive (even though the transfer involved the "processing" of data, and even though it was the airlines that arranged for the transfer of the data). The reason was that the processing of such data "*falls within a framework established by the public authorities that relates to public security*": see §58. *A fortiori,* in the context of the present case, processing of data involved in activities such as the transfer of bulk data to the SIAs (rather than to a foreign state), in particular for the purposes of national security, does not fall within the scope of the Data Protection Directive; nor equally can it engage the e-Privacy Directive.

23. The recent opinion of AG Mengozzi in *Opinion 1/15* [**SA/1/18**] on the draft agreement between Canada and the EU on the transfer and processing of PNR data is to similar effect. That Opinion concerns a draft agreement between the EU and Canada concerning the transfer of PNR data to the Canadian competent authorities[4]. AG Mengozzi cast no doubt upon the conclusion in *Parliament v Council* that the transfer of data in that case occurred within a framework established by public authorities that relate to public security, which did not come within the scope of the Data Protection Directive: see §85.

24. The same logic applies equally to the transfer of BCD and BPDs to the intelligence agencies. Such transfer of data takes place within a framework established by public authorities that relates to public security, and which therefore does not come within scope of the Data Protection Directive or e-Privacy Directive. Contrary to paragraph 23 of the Claimant's skeleton argument, section 94 does not "tacitly concede" the relevance of EU law: the requirement of proportionality was inserted to reflect the requirements of the ECHR.

25. The Respondents' response to this claim (as redacted and gisted for OPEN disclosure) [**Core/A/6**] confirms at §§7-16 that:

    25.1 Both GCHQ and MI5 acquire BCD from providers of electronic communications services (referred to variously as "communications servive providers" (CSPs) or "communication network providers" (CNPs)) pursuant to s.94 directions. The data received is retained and aggregated in a database held by GCHQ and MI5 respectively. The communications data provided by CSPs is limited to traffic data and service use information. This does not include communication content or subscriber information, and so cannot be ascribed to an individual, taken alone.

[4] Such an agreement by definition fell within the scope of EU law. Specifically, it was made on the basis of Article 82(1)(d) TFEU and Article 87(2)(a) TFEU, read in conjunction with Article 218(6)(a)(v) TFEU. Those provisions refer to police and judicial cooperation in criminal matters (and in the case of Article 218 for the making of international agreements by the EU). In the view of AG Mengozzi, the agreement ought also to be made on the basis of Article 16(2) TFEU.

25.2 GCHQ merges the data with its wider datasets, enriching the results of analytic queries made on those systems. Such analysis of BCD is vital for identifying and developing intelligence targets.

25.3 MI5 retrieves data from its database using sophisticated software, run against the data to answer specific investigative questions. Requests of the database can be made only where an authorisation is granted under a process akin to section 22 of RIPA, if judged necessary and proportionate.

25.4 The communications data is provided by CSPs on a regular basis. It is data which is maintained and retained by CSPs for their own commercial purposes (particularly billing and fraud prevention).

26. Section 94 directions therefore operate in a different way to retention notices under DRIPA. They do not require providers of electronic communication services to retain any data that they would otherwise not have retained. Nor do they require providers to process such data by searching their systems in order to retrieve and disclose information in response to specific requests for targeted requests. Instead, the only obligation on such providers is to transfer bulk communications data (without subscriber information) to GCHQ and MI5 respectively.

27. Similarly, in the case of BPDs, the SIAs collect datasets from a variety of sources, which are then incorporated into an analytical system and used and accessed for intelligence purposes. Although this may involve some data processing by a person other than state authorities, any such processing does not in itself fall within the scope of the Data Protection Directive, for the reasons identified by the court in *Parliament v Council*: they are inextricably bound up with the carrying out of the national security activities themselves.

28. Since the purposes for which the data is processed fall outside the scope of EU law, Charter rights are not engaged:

28.1 Article 6(1) TEU [**SA/1/1**] makes clear that "*The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties.*" Article 51(2) of the Charter further confirms that "*The Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties.*"

28.2 Moreover, Article 51(1) of the Charter [**SA/1/3**] makes clear that the provisions of the Charter are addressed to the Member States "*only when they are implementing Union law*". The s.94 and BPD regimes do not implement EU law.

It follows that Articles 7 and 8 of the Charter have no application to the present circumstances. The only test of the proportionality of the use of bulk data arises under Article 8 ECHR, and not under EU law.

(iii) The use of bulk data by law enforcement agencies

29. Further and in any event, even in the context of the fight against serious crime by law enforcement agencies (distinct from the field of national security), the use of BCD acquired under a s.94 direction and of BPDs falls outside the scope of the Directives. The Claimant is incorrect to suggest that *Watson* is authority for the proposition that any retention of or access to communications data or BPDs falls within the scope of EU law.

30. In *Watson* [**SA/1/17**], the CJEU recognised at §69 that Article 1(3) of the e-Privacy Directive excludes from its scope "*activities of the State*" in the areas of criminal law. The CJEU expressly drew an analogy with Article 3(2) of the Data Protection Directive, whose effect it had already considered in Case C-101/01 *Lindqvist* [**SA/1/8**] at §43 and Case C-73/07 *Satakunnan Markkinapörssi* at §41 [**SA/1/12**]. In those cases, the CJEU had confirmed that that by virtue of Article 3(2), the Data Protection Directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of EU law such as those listed, being "*activities of the State or of State authorities and unrelated to the fields of activity of individuals.*"

31. At §70 of *Watson*, the CJEU contrasted the effect of Article 1(3) of the e-Privacy Directive with that of Article 3, which sets out where the directive does apply – namely, to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices ("***electronic communications services***"). Consequently, the CJEU concluded, "*that directive must be regarded as regulating the activities of the providers of such services*" (emphasis added).

32. It is therefore apparent that, in the context of areas of criminal law, the CJEU drew a direct contrast between "*activities of the State*" falling within the specified fields on the one hand, which fall outside the scope of the e-Privacy Directive, and "*activities of the providers of electronic communications services*" on the other, to which the Directive directly applies. It was necessary for it to do so because, as Article 1(3) makes clear, it is only "*activities of the State*" in areas of criminal law which are excluded. The Respondents note that the same qualification is not imposed by Article 1(3) in the area of national security, where the exclusion is wider.

33. Against that background, the CJEU considered the effect of Article 15(1) of the e-Privacy Directive at §§71-74.

33.1 At §71, the CJEU noted that Article 15(1) specifically stated that Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Articles 5, 6, 8(1)-(4) and 9, including measures "*providing for the retention of data*".

33.2 At §72, the CJEU again confirmed the importance of the contrast between activities "*characteristic of States or State authorities*" and those which are "*unrelated to fields in which individuals are active*" (referring to Case C-275/06 *Promusicae,* which in turn referred back to *Lindqvist* at §43), noting that "*Admittedly, the legislative measures that are referred to in Article 15(1) of [the e-Privacy Directive] concern activities characteristic of States or State authorities"*, and noting the overlap of the objectives of such measures with those pursued by the activities referred to in Article 1(3) of the Directive.

33.3 At §73, the CJEU made clear that that tension could not be resolved simply by concluding that all such legislative measures were themselves excluded from the scope of the Directive: indeed, Article 15(1) necessarily pre-supposed that the legislative measures referred to fell within the scope of the directive (and would be deprived of any purpose if that were not the case).

33.4 At §74, the CJEU resolved the tension: it noted that the legislative measures referred to in Article 15(1) governed "*the activity of providers of electronic communications services*" (and not the activity of the State or of State authorities). Hence Article 15(1), read together with Article 3 (which, made clear that the Directive applies specifically to providers of electronic communications providers – see §70), must be interpreted as meaning that such legislative measures fall within the scope of the Directive.

34. At §§75- 80, the CJEU went on to consider whether, in consequence, the scope of the Directive extended not only to measures requiring the retention of such data, but also to the access of the national authorities to the data retained by the providers of electronic communications providers. As appears at §§65-66, the UK and the Commission had contended before the CJEU that only legislation relating to the retention of the data, but not legislation relating to the access to that data by the national authorities, fell within the scope of the Directive.

34.1 At §75, the CJEU confirmed that legislative measures requiring providers of electronic communications services to retain traffic and location data fell within the scope of the directive, since to retain such data necessarily involves the processing "*by those providers*" of personal data.

34.2 At §76, the CJEU stated that the scope of the Directive also extended to a legislative measure relating to the access of the national authorities to the data retained *"by the providers of electronic communications services"*. There were two reasons given for that conclusion.

(a) The CJEU stated at §§77-78 that a legislative measure under Article 15(1) requiring providers of electronic communications services to grant national authorities access to the data retained by those providers, notwithstanding the confidentiality of electronic communications and related traffic data guaranteed by Article 5 of the Directive, "*concerns the processing of personal data by those providers, and that processing falls within the scope of that directive"* (emphasis added).

(b) The CJEU stated at §79 that "*since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions of access by the competent national authorities to the data retained by the providers of electronic communications services"* (underlining added). At §80 it observed that that interpretation was confirmed by Article 15(1b) of the e-Privacy Directive, which made clear that providers were to establish internal procedures for responding to the requests for access to users' personal data.

35. The Respondents emphasise that the context in which all of these observations are made concerns:

35.1 traffic and location data which is retained by *providers* (not State authorities);

35.2 access to such data which is provided by the further processing of the data by the *providers* (not State authorities); and

35.3 data which is retained *only* for the purposes of such processing as subsequently required by national authorities, not data which is held for the commercial purposes of the providers themselves (and transferred in bulk to State authorities for their own use and access for the purposes of national security and/or other purposes specified by Article 1(3)).

36. None of those matters cast any doubt at all upon the principle that the e-Privacy Directive is concerned with the processing of personal data by service providers and not by State authorities (including retention and provision of access to such data) in areas of criminal law, which fall outside the scope of the Directive and of EU law. That is also consistent with the earlier conclusion of the CJEU in Case C-301/06 *Ireland v European Parliament and Council* [**SA/1/11**] that the provisions of Directive 2006/24 ("***the Data Retention Directive****"*), which amended the e-Privacy Directive, were "*essentially limited to the activities of service providers"*, to the exclusion of State activities coming under Title VI of the TEU (as it then stood, dealing with police and judicial cooperation in criminal matters): §§80-84. The CJEU did not refer to or qualify this decision in *Watson*, despite the fact that the referring court (the Court of Appeal) had specifically drawn attention to it: see *Davis and ors v SSHD* [2015] EWCA Civ

1185 [**SA/2/22**] at (among other places) §§56-58 and 95-96. Even if the CJEU's earlier conclusions on whether access to data retained by service providers fall within scope of the e-Privacy Directive have to be read as moderated in *Watson*, the essential finding that access to data or the use there of by the State authorities does not fall in scope is not affected in any way.

37. Nor do they cast any doubt upon the conclusion that the CJEU did not intend to lay down in its judgments in *Digital Rights Ireland* [**SA/1/14**] (or in *Watson*) any mandatory requirements applicable to national legislation on access to data that does not implement EU law: see the Court of Appeal's observations in *Davis* at §103 (as noted by CJEU at §57).

38. The result is that the use of bulk data under the s.94 and BPD regimes by law enforcement agencies falls outside the scope of the Directives also. No other approach provides any meaning to Article 1(3) of the e-Privacy Directive and Article 3(2) of the Data Protection Directive (and the Claimant gives them none). Even absent Article 4(2) TEU, the same would be true of the SIAs, who are self-evidently State authorities also.

(iv) Response to the Claimant's submissions on the scope of EU law and the Directives

39. The Claimant's submissions on the scope of EU law appear at §§32-46 of its skeleton argument of 15 May 2017. They focus largely on BCD, touching on BPDs only at §46 (and earlier at §§26-29).

- *BCD*

40. The Claimant's primary concern in its submissions on the scope of EU law is to establish that where a Member State restricts or interferes with a fundamental right or freedom which has been conferred on an individual by EU law, the fact that the Member State seeks to justify such interference by reference to the interests of public security does not take the matter outside the scope of EU law. Thus:

    40.1 at §34, the Claimant explains at some length that Member States must be able to establish to a national court the necessity and proportionality of a decision to restrict an EU citizen's freedom of movement, even if the decision to impose the restriction was on the grounds of public security; and

    40.2 at §42, the Claimant refers to the Floe Telecom litigation, in which it was established that the freedom to provide electronic communications networks and services could be restricted on the grounds of public security, with respect to the right of use of radio frequencies to the extent of requiring an individual licensing regime for the use of commercial multi-user GSM gateways.

41. In each example, it is the restriction of a pre-existing right or freedom conferred under the Treaties which falls within the scope of EU law. So much is uncontroversial. But it

does not follow that matters of national security fall within the scope of EU law (contrary to the express terms of Article 4(2) TEU): they do not. Still less does it follow that the matters at issue in the present case involve the restriction of any pre-existing right or freedom capable of engaging EU law.

42. The Claimants assert that section 94 directions interfere with the rights found within the e-Privacy Directive itself at Articles 5 and 6 in particular: see skeleton §§37(b) and (c). However, this simply begs the question as to the scope of the Directive, and thus as to the extent of the rights in fact conferred.

43. In fact, Article 5 confers no relevant right of confidentiality of BCD from their acquisition, retention and access by the intelligence agencies for the purposes of protecting national security in the first place: such activities are expressly stated to fall outside the scope of the Directive in Article 1(3). Article 5 therefore extends no relevant right with which the activities of the intelligence agencies could be said to be interfering. Nor does Article 6 apply to traffic data which is stored by the intelligence agencies.

44. A section 94 direction does **not** "*rewrite EU law and obligations of UK PCNs/PECSs"*, as the Claimant asserts at §44, therefore. Instead, the making of such directions is wholly consistent with the fact that the state's national security related activities fall outside the scope of EU law.

45. The Tribunal has therefore been presented by the Claimant with an argument that amounts to an extended effort to pull itself up by its own bootstraps.

46. Notably, the Claimant fails to engage with any of the Respondents' arguments as to the scope of the Directives, or as to the significance of the distinction drawn by the CJEU in *Watson* between the activities of the State and activities of providers of electronic communication services (as previously set out in section B of the Respondents' skeleton argument dated 2 March 2017, and repeated above).

47. The Claimant's contention (at skeleton §§20(c)) that a s.94 direction is "*materially identical*" to a DRIPA retention notice is incorrect. Unlike the position in relation to the DRIPA retention notices considered in *Watson*, a s.94 direction places no obligation on a *provider* of electronic communication services to retain data, or to search its systems in order to retrieve and disclose specific data in response to targeted requests. The Claimant's suggestion that the CJEU's judgment extends to all retention of data *by State authorities*, whether or not for national security purposes or for other specified purposes falling within Article 1(3) of the e-Privacy Directive or Article 3(2) of the Data Protection Directive, is incorrect.

48. Notably, the Claimant does recognise at §§35(a), 37(a) and §45 of its skeleton argument that certain national security activities do fall outside the scope of the Treaties and of the Directives. In particular, at §45 the Claimant concedes that "*free-standing*

activities" including the "*interception of communications without compulsion or assistance from a PCN/S"* do not engage EU law. That concession is correct, so far as it goes. But it is incorrect insofar as it is suggested that a direction under section 94 in and of itself brings the acquisition of communications data within the scope of EU law, by reason of an element of compulsion or assistance. The transfer of BCD to the intelligence agencies takes place within a framework established by public authorities that relates to national security, and for that reason (as explained in *Parliament v Council*, supra) falls to be considered as an activity of the intelligence agencies themselves, outside the scope of EU law and of the Directives.

49. It is necessary also to address a number of discrete points made by the Claimant.

50. **Firstly**, at §40 of its skeleton argument, the Claimant mischaracterises the Respondents' answer to a question from the Tribunal as a "*concession … that a section 94 Direction requires processing just as a DRIPA retention did*" and that "*This engages the rights and harmonised obligations in the e-Privacy Directive (in this case both Article 5 and Article 6(5)."* That is incorrect. The Respondents accept only that *if* the Directives were to apply to such activities, the transfer of BCD to the intelligence agencies would amount to "*processing*" within the definition of Article 2(b) of the DPD. That is explicitly <u>not</u> a concession that such activities fall within the scope of the Directives or that they engage the rights and obligations in the e-Privacy Directive.

51. **Secondly**, the Claimant also seeks (at skeleton §§20(b)) to extend the effect of §73 of the CJEU's judgment to the national security context. However, §73 cannot be read as suggesting that any national measures on national security may fall within the scope of the e-Privacy Directive simply by virtue of the reference to "*national security*" in Article 15(1):

    51.1 That would be inconsistent with primary law, namely Article 4(2) TEU.

    51.2 In any event, the Claimant ignores §74, which makes clear that "*the legislative measures referred to in Article 15(1) govern, for the purposes mentioned in that provision, the activity of <u>providers</u> of electronic communications services.*" Article 15(1) plainly does not refer to legislative measures which govern the activities of the State authorities concerning national security, or any other activities which are so closely connected with the State's activities that they form part of the "*framework"* of national security (as the term was used in *Parliament v Council*): in each case, those matters fall outside the scope of the Directive by virtue of Article 1(3), with the result that Article 15(1) can have no application to them. Just as the court recognised that the activities of State authorities in the area of criminal law remained out of scope of the Directive notwithstanding the terms of Article 15(1) (see §69), the same is true of activities falling within the national security framework.

51.3 The reference to "*national security*" in Article 15(1) of the Directive makes clear that legislative measures may be taken to restrict the rights and obligations referred to where necessary, appropriate and proportionate to safeguard national security *even where* the Directive *is* engaged.

52. **Thirdly**, the Tribunal is not assisted by the Claimant's suggestion (at skeleton §43) that the Respondent's submissions on these points amount to a "*collateral attack*" on the validity of the judgment in *Watson*, or amount to an abuse of process. The points set out above were not determined in *Watson.*

53. **Fourthly**, the Claimant is also incorrect (at skeleton §43(a)) in its account of the arguments advanced by the UK before the CJEU, which were materially different: in particular, they took as their starting-point that the retention of communications data by service providers under a DRIPA retention notice fell within the scope of EU law. The CJEU's conclusion that access to such retained data also fell within the scope of EU law depended upon the fact that retention of such data by service providers for the purposes of access already engaged EU law, and that provision of access by the service providers amounted to a further act of data processing by them: see *Watson* at §§78-79. There is no equivalent retention or provision of access by service providers in the present case.

54. **Fifthly**, the Claimant contends (at skeleton §§43(b)-(f) and 71) that DRIPA was "*national security legislation"* and that it is wrong to suggest that DRIPA and *Watson* were about criminal investigation alone; and that the CJEU had "*tailored its judgment to national security cases",* which is said to be "*fatal to the Respondent's argument that national security retention was not being considered in Watson".* In substance, beyond the arguments on scope already set out above, this argument is based upon the final sentence of §119 of the judgment alone. However, in §119, the reference to national security arises explicitly in the context of "*objective of fighting crime*" (in the second sentence): the subsequent reference to national security arises only in relation to a subset of crime, namely in a "*specific case"* of "*terrorist activities*", where wider access to data might be granted other than that of a suspect. National security activities are otherwise ignored in the analysis, and play no part in the *dispositif* – with good reason, as they fall out of scope. There is therefore no analysis at all of national security activities such as nuclear counter-proliferation, defence against cyber-attacks or interference with elections by a hostile state, support of troops in an armed conflict abroad, counter-espionage, or even counter-terrorism in its national security aspect (rather than purely criminal aspect).

55. **Sixthly**, the fact that BCD acquired by the SIAs for national security purposes under a s.94 direction may be shared (pursuant to s.19(2), (3) and (5) of the Counter-Terrorism Act 2008 [**A/1/9**]) for use for other purposes, such as the detection of serious crime, does not alter the analysis. The transfer of such data, after its acquisition, for the purpose of criminal investigation falls outside the scope of the e-Privacy Directive (by virtue of Article 1(3)) as it would at that stage relate to "*the activities of the State in*

areas of criminal law": it does not matter that it is used for purposes other than protecting national security.

- *BPDs*

56. The Claimant claims (at skeleton §§26 and 46) that the obtaining of BPDs engages EU law pursuant to the Data Protection Directive. It is vague as to how that might be so. It appears to suggest that the fact that the intelligence agencies might "*mandatorily co-opt private commercial actors … to provide such a database, EU law is engaged, whether through the Data Protection Directive or through general EU law principles."* However, the Claimant does not identify which provision or provisions of the DPD are said to have that result, and points to no equivalent to Articles 5 or 6 of the e-Privacy Directive (upon which it relies for the purposes of its arguments on BCD).

57. In view of the weakness of that position, the Claimant refers to "*those working in a field engaging free movement rights*" such as an airport operator, and suggests that a direction to such an operator to provide BPDs "*will be a relevant restriction within the meaning of the DPD".* But what restriction "*within the meaning of the DPD*" is in play is left entirely obscure.

58. The correct position is rather that the obtaining of BPDs within the framework of national security does not engage EU law (see Article 4(2)) or the Directive (see Article 3(2) of the Directive and *Parliament v Council*, supra).

C. Retention of BCD and BPDs by the SIAs is lawful

59. The Claimant's bald assertion (at skeleton §21) that it was held in *Watson* that large-scale bulk retention of BCD is unlawful under EU law is incorrect. In *Watson,* the CJEU considered (in the context of the *Tele2 Sverige* reference) only the lawfulness of the imposition:

    59.1 of a requirement on service providers

    59.2 for the general and indiscriminate retention of communications data

    59.3 which they would not otherwise have retained for any commercial or operational purpose

    59.4 for the purpose of fighting crime.

60. As to the **first** of those points, the issue of retention of data by *service providers* does not arise in the case of s.94 directions: such directions do not require service providers to retain any data.

61. As to the **second**, the complaint about the general and indiscriminate retention of communications data related only to the Swedish position, not that in the UK.

62. As to the **third**, neither the s.94 regime nor the BPD regime imposes any requirement on any individual to retain data. Any data with which the BPD regime is concerned relates to data lawfully held for the purposes of the activities of the data owners concerned.

63. As to the **fourth** of those points:

    63.1 The Swedish legislation in question provided for the retention of communications data so that it could be accessed by national police, the Swedish Security Service and Swedish Customs Authority in order to avert, prevent or detect criminal activity involving any offence punishable by imprisonment for over 2 years, and certain specified offences punishable by a lesser term of imprisonment. The retained data was also required to be disclosed to the prosecution authority, police, Security Service or other public law enforcement authority if the data was connected with any presumed criminal offence. National authorities could also place a person under surveillance in respect of the preliminary investigation of offences punishable by imprisonment for at least six months: see *Watson* at §§22, 25, 26.

    63.2 The first question referred to the CJEU expressly made clear that the legislation was sought to be justified "*for the purpose of combating crime*", and was addressed by the court on that basis: §§51, 62.

64. As set out above and by contrast, the retention of data by the SIAs for the purpose of national security falls outside the scope of EU law and is accordingly lawful if authorised by domestic legislation and otherwise compatible with the ECHR. Further, the retention of data *by State authorities* for any purpose falling within Article 1(3) of the e-Privacy Directive and/or Article 3(2) of the Data Protection Directive falls outside the scope of EU law. *Watson* is not authority to the contrary. It follows that the s.94 regime and the BPDs regime are materially different from the position considered by the CJEU in *Watson.*

D. The safeguards identified in *Watson* are neither necessary nor appropriate to ensure the proportionality of access to BCD and BPDs, in particular in national security cases

65. The Claimant asserts that the use of BCD acquired under a s.94 direction and BPDs lack safeguards which are mandatory under EU law, namely:

    65.1 a requirement for independent authorisation for access;

65.2 procedures for notification of use of the data;

65.3 adequate controls on how they are shared; and

65.4 a prohibition on the transfer outside of the EU.

66. Even if EU law were engaged and the Directives applied (which they do not), it would not follow that such safeguards are required in the case of the acquisition and use of BCD under a s.94 direction and BPDs. The Claimant's submission ignores:

66.1 the proper approach to the assessment of proportionality and the breadth of discretion afforded to Member States on matters of national security;

66.2 the context in which the SIA use bulk data, and in particular the difference in purpose and nature of access to BCD obtained under a s.94 direction and to BPDs (none of which was in evidence before the CJEU in *Watson*);

66.3 the impact that that difference has on the appropriateness of and necessity for the safeguards identified in *Watson*.

67. When the nature and purpose of such access is assessed in its proper context, it is apparent that the "safeguards" proposed by the Claimants are neither necessary nor appropriate. Alternative safeguards are in place which are suitable and proportionate to the circumstances of the nature of the data in question and of the use to which the data are put.

(i) The proper approach to the proportionality assessment and margin of appreciation

68. The proportionality assessment is a fact-sensitive one, for the national court to apply. As it was put by Lord Reed and Lord Toulson JJSC in *R (Lumsdon) v Legal Services Board* [2016] AC 697 [**SA/2/23**] at §§29-30:

> *"29. On the other hand, when the validity of a national measure is challenged before a national court on the ground that it infringes the EU principle of proportionality, it is in principle for the national court to reach its own conclusion. It may refer a question of interpretation of EU law to the Court of Justice, but it is then for the national court to apply the court's ruling to the facts of the case before it. The court has repeatedly accepted that it does not have jurisdiction under the preliminary reference procedure to rule on the compatibility of a national measure with EU law: see, for example, Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano (Case C-55/94) [1996] All ER (EC) 189, para 19. It has explained its role under that procedure as being to provide the national court "with all criteria for the interpretation of*

Community law which may enable it to determine the issue of compatibility for the purposes of the decision in the case before it": Gebhard , para 19.

30. Nevertheless, where a preliminary reference is made, the Court of Justice often effectively determines the proportionality of the national measure in issue, by reformulating the question referred so as to ask whether the relevant provision of EU legislation, or general principles of EU law, preclude a measure of that kind, or alternatively whether the measure in question is compatible with the relevant provision of EU legislation or general principles. That practice reflects the fact that it can be difficult to draw a clear dividing line between the interpretation of the law and its application in concrete circumstances, and an answer which explains how the law applies in the circumstances of the case before the referring court is likely to be helpful to it. The practice also avoids the risk that member states may apply EU law differently in similar situations, or may be insufficiently stringent in their scrutiny of national measures. It may however give rise to difficulties if the court's understanding of the national measure, or of the relevant facts, is different from that of the referring court (as occurred, in a different context, in Revenue and Customs Comrs v Aimia Coalition Loyalty UK Ltd (formerly Loyalty Management UK Ltd) [2013] 2 All ER 719)."

69. The last sentence of §30 is prescient. It is particularly to be borne in mind when the principles identified in one context are sought simply to be transposed into another context involving *different* facts. Moreover, this Tribunal is well placed properly to understand the present context and the work of the SIAs.

70. Further, on the hypothesis that the effect of Article 4(2) TEU was not to exclude national security from the scope of EU law, its effect would still be that Member States have the broadest possible margin of appreciation in the field of national security, including in designing systems for collecting, retaining and accessing data. Article 4(2) TEU confers a special status on national security matters, which it is not for the EU institutions (including the CJEU) to assess. Given that national security remains the "*sole responsibility*" of each Member State, only the Member State is in a position to assess the seriousness of the threats that it faces, and hence the necessity of using bulk data to assist in averting those threats, in particular by identifying the individuals who present them. It also remains for the national authorities to consider the effectiveness of the measures adopted in the interests of national security. That has inevitable implications for any assessment of the proportionality of any measures introduced on grounds of national security: cf. *R (Lord Carlile of Berriew QC) v SSHD* [2015] AC 945 [**SA/2/21**], at §§19-38. Although the court is ultimately responsible for the assessment of proportionality, that exercise must be undertaken on the basis that a Member State's authorities responsible or national security have particular wide discretion as to what is required.

(ii) Difference in purpose and nature of access and use

71. Neither access to BCD acquired under a s.94 direction nor the acquisition or access to BPDs are properly comparable to the DRIPA regime. There are (at least) four important differences.

72. **First**, bulk data (whether BCD or BPDs) is used *inter alia* to identify, understand and disrupt threats to national security. For example, bulk data can be used to discover and identify individuals who may not previously have been known to the security and intelligence agencies, but who may be so identified by the application of complex analysis, automated processing and scenario tools or predetermined assessment criteria to the bulk datasets held (in combination with each other). That is a fundamentally different use to the circumstances contemplated by the court in *Watson* at §§111 and 119, which took as their starting point only that data relating to specific individuals who were under investigation in respect of a specific criminal offence (whether already committed or in the planning) could be retained and accessed on a targeted basis. That is not how the process of target identification works, or could possibly work.

73. **Second**, under the DRIPA regime (as under the Swedish laws discussed in *Tele2 Sverige* [**SA/1/17**]), the service providers were required to retain data for which they had no further commercial use. The sole purpose of retention was to ensure that data that would not otherwise be held by a CSP for business purposes is available to be accessed and disclosed to the authorities on request. That is not the position in the bulk data regime. The difference is significant:

    73.1 Compare the opinion of AG Mengozzi in *Opinion 1/15* [**SA/1/18**] at §§178-179, relating to the draft agreement on the transfer and processing of PNR data by air carriers flying between Canada and the EU. While the Advocate General considered the draft agreement to infringe the EU Charter on other grounds, he concluded that the collection of PNR data by air carriers did not entail any interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter because the airlines were already engaged in the collection of such data for their business purposes. See further *Watson* at §§86 and 92.

    73.2 See also *Watson* at §79, where it was made clear that it was because data was retained *only* for the purpose, when necessary, of making that data accessible to the competent national authorities, that the fact that the national legislation in question imposed the retention of data necessarily entailed the existence of provisions relating to access by the competent national authorities to the data retained.

74. **Third**, so far as BCD acquired under a s.94 direction is concerned, the data omits subscriber information, distinguishing the position from that described in *Watson* at §98 (although the data may be used to identify a person in combination with other datasets, depending on their content).

75. **Fourth**, so far as BPDs are concerned, the Claimant appears to assert that the Data Protection Directive is equivalent in effect to the e-Privacy Directive. It is not. There are significant differences:

75.1 So far as the e-Privacy Directive is concerned, it imposes an obligation of confidentiality on CSPs in respect of matters within its scope (Article 5), and then provides for derogations in certain circumstances (Article 15) [**SA/1/5**]. In *Watson,* the CJEU was considering the requirements of necessity, appropriateness and proportionality for legislation falling within that derogation.

75.2 The Data Protection Directive operates differently. Article 1 states that "*In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data*" [**SA/1/4**]. This aim is then achieved through the text of the Directive. The Directive imposes no similar obligation of confidentiality comparable to that in Article 5 of the e-Privacy Directive, and to which the Article 15 derogation attaches. Instead, Article 6 (principles relating to data quality) requires Member States to provide that personal data must be (in summary):

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and kept up to date; and

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

75.3 Article 7 provides that personal data may legitimately be processed if, among other things, (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).

75.4 Article 13 provides for exemptions and restrictions, in that Member States may adopt legislative measures to restrict the scope of the obligation and rights provided for in Article 6 (among other Articles, but not Article 7), when such a restriction constitutes a necessary measure to safeguard any of the identified objectives (including national security, defence, public security and the fight against crime, amongst other matters).

76. Even if (which is denied) the Data Protection Directive were engaged by the BPD regime, the processing of BPDs would nonetheless fall within Article 7(e) of the Data Protection Directive, for which no derogation under Article 13 is either available or required.

77. Taken in combination, the above matters have a significant impact on the necessity for and appropriateness of safeguards for the use of such data in order to ensure compatibility with rights under Article 7 and Article 8 of the Charter.

(iii) Significance of difference for appropriateness of safeguards

78. In *Watson,* the CJEU identified safeguards at §§119 to 122 which it thought appropriate to the circumstances of the use of retained data in the targeted investigation of serious crime. In so deciding, it drew on its previous judgments in *Digital Rights Ireland* [**SA/1/14**] at §§62-68 and *Schrems* [**SA/1/15**] at §95, which it considered applied by analogy in the context of the traffic and location data retention regimes at issue.

79. However, in *Opinion 1/15* [**SA/1/18**], AG Mengozzi recognised that a different approach to safeguards than that adopted in *Digital Rights Ireland* and *Schrems* was appropriate in the case of the provision of bulk PNR data to the Canadian authorities, in light of the different nature of the activity and the purpose of threat identification served. Thus:

79.1 At §205, AG Mengozzi recognised that the envisaged agreement between the EU and Canada was capable of attaining the objective of public security as a means of threat identification:

> *"… I do not believe that there are any real obstacles to recognising that the interference constituted by the agreement envisaged is capable of attaining the objective of public security, in particular the objective of combating terrorism and serious transnational crime, pursued by that agreement. As the United Kingdom Government and the Commission, in particular, have claimed, the transfer of PNR data for analysis and retention provides the Canadian authorities with additional opportunities to identify passengers, hitherto not known and not suspected, who might have connections with other persons and/or passengers involved in a terrorist network or participating in serious transnational criminal activities."*

79.2 At §§215-216, he emphasised again that:

> "*215. It is the case that those categories of PNR data are transferred to the Canadian travellers for all travellers flying between Canada and the Union even though there is no indication that their conduct may have a connection with terrorism or serious transnational crime. 216. However, as the interested parties have explained, the actual interest of PNR schemes, whether they are adopted unilaterally or form the subject matter of an international agreement, is specifically to guarantee the bulk transfer of data that will allow the competent authorities to identify, with the assistance of automated processing and scenario tools or predetermined assessment criteria, individuals not known to law enforcement services who may nonetheless present an 'interest' or risk to public security and who are therefore liable to be subjected subsequently to more thorough individual checks.*"
>
> He added at §241: "*Those checks must also be capable of being carried out over a certain period after the passengers in question have travelled.*"

79.3 The difference in nature and purpose of the data was relied upon by the Advocate General to explain why safeguards thought applicable in the context of the Data Retention Directive in *Digital Rights Ireland* (and subsequently to national measures in *Watson*) did not apply in the same way. Thus:

(a) Although in the case of data retention, the court has expressed the view that indiscriminate retention of all data is unlawful and that a more targeted approach is required (including by geographical area), he rejected that approach in the context of bulk PNR data: see §244. Selective acquisition of such data would not be effective:

> *"No other measure which, while limiting the number of persons whose PNR data is automatically processed by the Canadian competent authority, would be capable of attaining with comparable effectiveness the public security aim pursued by the contracting parties has been brought to the Court's attention in the context of the present proceedings."*

(b) Although in the case of data retention, the court has expressed the view that prior authorisation by a court or independent administrative body should be required before retained data is acquired from a CSP, at least in the targeted investigation of serious crime, he rejected that approach in the context of bulk PNR data at §269:

"the appropriate balance that must be struck between the effective pursuit of the fight against terrorism and serious transnational crime and respect for a high level of protection of the personal data of the passengers concerned does not necessarily require that a prior control of access to the PNR data must be envisaged."

(c) So far as post-factum judicial oversight of the measures was concerned, he considered it sufficient that Article 14(2) of the draft agreement (COM (2013) 528 final) provided that Canada was to ensure that any individual who was of the view that their rights had been infringed by a decision or action in relation to their PNR data may seek effective judicial redress in accordance with Canadian law by way of, inter alia, judicial review: see §271. He emphasised that in those circumstances the lack of prior authorisation for access was consistent with the ECtHR's jurisprudence: §270.

(d) A requirement that the data be kept within the EU did not arise. To the contrary, the whole purpose of the agreement was to allow for the appropriate sharing of the data outside the EU. There is no suggestion that such transfer is antithetical to EU law in principle. That is unsurprising: §122 in *Watson* is concerned with the security and protection of data retained by providers of electronic communications services, not with the use of such data once it has been accessed by the national authorities. Those uses must inevitably be international in nature, given the international threat to national security and the need to liaise closely with other trusted countries' intelligence services in order to meet that threat.

80. The EU-Canada agreement was justified on the grounds of the fight against terrorism and serious transnational crime. However, additional matters arise in the context of national security, rendering the data retention safeguards identified in *Watson* even more inappropriate in that context. In particular, the work of the security and intelligence agencies must be conducted in secret if it is to be effective in achieving its aims. The value of intelligence work often relies on an identified target not knowing that his activities have come to the attention of the agencies, and/or not knowing what level of access to his activities the agencies have achieved. The requirement to notify a suspect of the use of bulk data tools against him, simply on the grounds that investigations have been concluded, would fundamentally undermine the work of the agencies. It may also threaten the lives of covert human intelligence sources (CHIS) close to him, such as a source who has provided the target's telephone number or email address to the agencies. In the context of national security, therefore, it is unsurprising that Article 346(1)(a) TFEU stipulates that "*no member state shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security.*" In those circumstances, the Claimant's assertion that the requirement for

notification in *Watson* can simply be read across to a national security case is clearly wrong.

81. Evidence has been prepared explaining the real distinctions between the use of bulk data by the SIAs in their work (as compared to a targeted police investigation which seems to have been at the forefront of the CJEU's mind in *Watson*). Those distinctions indicate plainly both (a) that the CJEU cannot be taken to have considered still less ruled on a context such as the present in *Watson*; and (b) that decisions as to the nature of safeguards have to take into account the context in which they are to operate. The evidence goes on to explain why the safeguards identified in *Watson* could not practicably or effectively be adopted in the context of bulk data, see the third witness statement of the GCHQ witness dated 2 March 2017 [**Supp/11**].

82. It follows that the identified safeguards cannot sensibly be applied in the context of national security, nor to the use of BCD obtained under a s.94 direction or of BPDs. Instead, a bespoke set of safeguards, suitable and appropriate to the circumstances of the case, is required. The safeguards in place have been set out in the OPEN versins of the witness statements of each of the GCHQ, Security Service, and SIS witnesses. For the reasons set out under the heading of "Proportionality" below, the net effect of the safeguards, taken with the importance and value of the use of such data to protect the United Kingdom's national security, is that the regime for the use of BCD and BPDs is proportionate.

E. The Claimant's submissions on the scope of *Watson* and EU competence

83. The Claimant previously contended that the s.94 and BPD regimes are unlawful because there is no mechanism to ensure that BCD acquired under a s.94 direction or BPDs are used only for the purpose of fighting serious crime. It has now abandoned that point, which was in any event inconsistent with the argument—which it maintains—that *Watson* concerns the use of data both to combat serious crime and for national security purposes and that there is no distinction between the two for the purposes of applying EU law (Claimant's skeleton, §68).

84. As already set out in **Sections B and C** above, the CJEU confined its judgment in *Watson* to issues concerning the retention of and/or provision of access to data by electronic communications service providers for the purposes of the investigation, detection and prosecution of serious crime. This was as far as it was necessary for the CJEU to go in order to address the questions referred by the Swedish Court in *Tele2* and by the Court of Appeal in *Watson*.

85. Moreover, for the reasons set out in **Section D** above, even if EU law were engaged and the Directives applied, the safeguards identified in *Watson* are not applicable to the acquisition and use of BCD under a s.94 direction and BPDs.

86. In their 10 May 2017 Outline Response to the Tribunal's Questions of 8 March 2017 the Respondents set out what their position would be if, contrary to the submissions above, the Tribunal were to find that the CJEU in *Watson* purported to make findings in relation to the retention of and/or access to databases held by the intelligence agencies for the purposes of national security.

87. The CJEU had no jurisdiction to make such findings, in the light of Article 4(2) TEU and the non-conferral of competence on the EU in relation to national security, and having regard to the nature of the questions that were before it. The CJEU has no jurisdiction to review or rule upon the actions of national intelligence agencies in acquiring and accessing BCD or BPD. To the extent that it may have appeared to do so, the CJEU would appear to have overstepped the jurisdictional limits set out in the European Treaties.

88. Insofar as there is any suggestion of such findings in the CJEU's judgment, the Respondents submit as follows:

    88.1 Any ambiguity as to the scope of the judgment must be read to avoid the conclusion that the CJEU, *contra legem*, assumed a jurisdiction it does not have. The judgment in *Watson* does not consider Article 4(2) TEU and its effects, does not seek to address the issues as to jurisdiction that Article 4(2) entails, and does not contain any clear indication that the CJEU intended to make findings in relation to the national security activities of the Member States notwithstanding the clear words of Article 4(2).

    88.2 The CJEU's judgment therefore can and should be read and applied consistently with the limits of the jurisdiction conferred on the EU by the Treaties, and therefore on the CJEU, by the Treaties. To the extent that there are alternative possible interpretations of the language in the judgment, reading it consistently with the fundamental provisions of the Treaties, to avoid treating it as an apparent *ultra vires* act, is in accordance with the principles of sincere cooperation, mutual loyalty and respect governing the relationship between national courts and the CJEU.[5]

    88.3 Interpreting the judgment in that way is also consistent with the principle of proportionality, whereby the content and form of any act of the EU shall not exceed what is necessary to achieve the objectives of the Treaties.[6] The CJEU simply did not need to make, and therefore can be assumed not have made, any findings in relation to the retention of or access to data by the intelligence agencies for the purposes of national security, particularly when its

[5] Cf. the approach of the German Federal Constitutional Court in its judgment of 24 April 2013 on the Counter-Terrorism Database (1 BvR 1215/07) at §91, in English at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2013/04/rs20130424_1bvr121507en.html [**2SA/49**]

[6] See Article 5(4) TEU.

conclusions are so clearly expressed as referring to national legislation in the context of fighting crime.

89. If, notwithstanding those considerations, the Tribunal considers that the CJEU's judgment in *Watson* is incapable of being read consistently with the limits of EU competence set at the European Treaty level, the Tribunal should make a reference to the CJEU pursuant to Article 267 TFEU to clarify the CJEU's position.

    89.1 Where a national court has legitimate doubts as to the validity of an act of the EU institutions, the principles of sincere cooperation and mutual respect again dictate that the proper course, in the first instance, is to make a reference to the CJEU to enable that Court to clarify its position. Article 267 TFEU establishes such a procedure for direct cooperation between the CJEU and the courts of the Member States.[7]

    89.2 Such reference would be necessary in any event since the conclusion that the CJEU has in *Watson* sought to apply the EU charter to the activities of the UK intelligence agencies would on no conceivable view be *acte clair*. Before any such conclusion could be reached by the Tribunal it would be necessary for there to be a reference to the CJEU to determine if that Court was truly purporting so to act.

90. If, in response to a request for clarification, the CJEU were unambiguously to confirm that it intended to apply the EU Charter to the use of data by the United Kingdom's intelligence agencies for the purposes of national security, notwithstanding the non-conferral of such competence on the EU, a difficult and novel question of some constitutional importance would arise as to the proper course for a domestic court to take faced with a judgment of the CJEU that manifestly exceeds its jurisdiction under the EU Treaties. That issue was considered by Lord Mance in *Pham* [2015] 1 WLR 1591 [**2SA/35**] at §§75ff.

91. As Lord Mance (and the other members of the Court who agreed with him) noted, especially at §76, the question for a United Kingdom court would be one of pure domestic law. It would relate to the meaning and effect of the European Communities Act 1972. As such, the question is one that could only be determined by the domestic courts; and would ask: what degree of sovereignty was ceded, or did Parliament intend to cede, to the Common Market and to the European Court? The stages of the argument, as Lord Mance's judgment indicates, would be along the following lines:

    91.1 It would be surprising if Parliament had intended to cede to the European Court, as Lord Mance put it at §90, "*unlimited as well as unappealable power to determine and expand the scope of European law*". That would represent, in a context in which the extent of cession of sovereignty has from the outset been highly controversial, an open ended cession. Ascribing such an intention

[7] See Case C-62/14 *Gauweiler* [**2SA/23**] at §15 and the AG's Opinion at §64.

to Parliament would have to survive being tested against extreme scenarios in which there is a clear departure from expressly agreed competence or jurisdictional limits. Only the clearest possible words would be capable of indicating such an intention. There is nothing approaching that clarity of expression in the 1972 Act.

91.2 Lord Mance specifically considered the reach of s.3(1) of the 1972 Act [**2SA/8**]. He acknowledged that the language was broad. The "*meaning or effect of any of the Treaties*" is to be treated as a "*question of law"*; and, if not referred, determined as such *"in accordance with the principles laid down by and any relevant decision of the European Court"*. He acknowledged that, "*on one reading, they leave the scope of the Treaty within the sole jurisdiction of the Court of Justice as a question as to its "meaning or effect".* However, he acknowledged that, even as a matter of language, that was only one reading. In any event, he evidently considered that, even if arguments could be made that that was the natural first reading, there were "*jurisdictional limits on the extent to which [the section] confers competence on the Court of Justice*" (§82). He cited, but merely as an example, the *Buckingham County Council* case [**2SA/32**] in which there was potential for conflict between EU law and Article 9 of the Bill of Rights.

91.3 He considered that it was entirely possible and coherent to distinguish between the meaning and effect of the Treaties on the one hand, and questions going to the competence and jurisdiction of the EU and its institutions, including the Court of Justice. As he put it: "*Questions as to the meaning and effect of treaty provisions are in principle capable of being distinguished from questions going to the jurisdiction conferred on the European Union and its court under the Treaties"*: §82.

91.4 As he noted, the constitutional nature of the 1972 Act and the particular context in which it was enacted are relevant, playing directly into the question of what Parliament intended in enacting s.3(1) of the 1972 Act. The specific features of the context which are of importance in the present context, and which Lord Mance evidently regarded as being of importance in the context of *Pham*, are, first, that the Treaties represent a cession of sovereignty. As Lord Mance described it "*the principle of conferral*" (§83) is in play. A deliberate, careful delineation of those areas within and without competence – where there has and has not been conferral – has been made by the Member States. That is done, for relevant purposes, and the principle of conferral is "*enshrined*" (§83) in Articles 4 and 5 TEU. These matters led, in the argument identified and developed by Lord Mance (and the other Justices), to the conclusion that Parliament had not intended to confer on the Court of Justice unlimited and unappealable power to expand its own jurisdiction; and it was thus for the domestic courts, as a matter of interpretation of the domestic

legislation read alongside the Treaties, to determine the scope of the conferral intended by Parliament.

91.5 Lord Mance posed his argument in the context in which there are jurisdictional limits "*clearly agreed"* (§90) in the Treaties. It is understandable that he should do so because that assumption casts the issues he was addressing into sharp relief. The issue whether that clarity, or some degree of clarity, is a precondition to the application of the principles he set out is moot. It is submitted that it does not need to be determined in this case. The fact is that the very provisions dealing with conferral and the limits of competence and jurisdiction addressed national security, and provided in Article 4: "*national security remains the sole responsibility of each member state*."

92. It is not necessary for the Tribunal to deal with this question, and these matters, now. First, because in accordance with the submissions set out above the CJEU did not, and did not purport to, address matters outside its competence, and to the extent that there is any ambiguity the judgment should be read consistently with the scope of EU law as conferred by the Treaties. Secondly, because the outcome of any reference to the CJEU cannot be prejudged, bearing in mind the principle of sincere cooperation and the need for dialogue between the national and EU courts to resolve any difficulty in interpreting and applying the *Watson* judgment.

F. Sharing of BPD/BCD

94. In its October 2016 judgment, and 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*." [**SA/2/24/§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)).

The law

95. As the Tribunal held at §37 of its judgment in *Liberty/Privacy* [**A/2/38**], 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*[8], at §78, quoted at §37 of *Liberty/Privacy*.

96. 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*[9] (at §§67-68m), *Leander v Sweden*[10] at §51 and *Esbester v UK*[11], quoted at §§38-39 of *Liberty/Privacy*. Thus, as held by the Tribunal in the *British Irish Rights Watch* case[12] (a decision which was expressly affirmed in the *Liberty/Privacy* judgment at §87): "*foreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security...*" (§38)

97. 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).

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

98.1. 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*[13] at §156 and its anticipated approval in *Liberty v United Kingdom*[14] at §68 (see §118 of *Liberty/Privacy* and also *Silver v United Kingdom*[15]).

98.2. 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:

[8] Appl. no. 4378/02, 21 January 2009 [**A/3/57**].
[9] (1984) 7 EHRR 14 [**A/3/46**].
[10] [1987] 9 EHRR 433 [**A/3/47**].
[11] [1994] 18 EHRR CD 72 [**A/3/49**].
[12] IPT decision of 9 December 2004 [**A/2/33**].
[13] [2011] 52 EHRR 4 [**A/3/59**].
[14] [2009] 48 EHRR [**A/3/55**].
[15] [1983] 5 EHRR 347 [**A/3/45**].

"*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."

98.3. 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 Intelligence Services Commissioner and the Interception of Communications Commissioner.

99. 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*[16], 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*[17] at §59)

100. 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*

[16] (2008) 46 EHRR SE5 [**A/3/53**].
[17] (1999) 28 EHRR [**A/3/50**].

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)

101. 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:

101.1. 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/3/59**] 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.

101.2. 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.

101.3. 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.

101.4. 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 and LEAs

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

102.1. GCHQ's Amended OPEN statement of 6 March 2017 [**Supp/7**];

102.2. Security Service's OPEN Statement of 10 February 2017 [**Supp/8**], together with a further OPEN statement dated 10 April 2017 [**2Supp/9**]; and

102.3. SIS's Amended OPEN Statement of 3 March 2017 [**Supp/9**].

103. The SIAs can neither 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: 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.

104. The Claimant contends that GCHQ has now avowed that it shares BPD with the 5-Eyes partners (Claimant's skeleton, §83) (although, for avoidance of doubt, no such argument is made in respect of BCD, or SIS and MI5).

105. This contention is incorrect as a consideration of the documents relied on by the Claimant (skeleton, §§82-83) reveals:

105.1. The term *"Sigint and non-Sigint data"*, which is quoted by the Claimant (skeleton, §82), 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.

105.2. 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.

105.3. 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.

106. The Claimant relies (skeleton, §83) 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:

106.1. 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 <u>never</u> 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.

106.2. The second document is David Anderson QC's Bulk Powers Review of August 2016 [**SA/2/27**]. 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.

107. 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, §83) 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.

108. As to the matters set out at §84 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.

109. 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.

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

110.1. 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)

110.2. 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).

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

110.4. 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).

110.5. 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).

110.6. 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)

110.7. 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).

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

110.8.1. Carrying out information gathering exercises, including into:

110.8.1.1. The nature of the proposed recipient;

110.8.1.2. The legal and policy regime that would apply in relation to BPDs in the recipient;

110.8.1.3. 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;

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

110.8.3. Individual consideration of each BPD to be shared and the terms of handling instructions to accompany each BPD shared.

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

110.8.5. Ending sharing with a recipient if judged necessary;

110.8.6. 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.

110.9. 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.

110.10. Disclosure of the whole or a subset of a BPD is subject to internal authorisation procedures in addition to those which apply to an item of data. 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).

110.11. 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).

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

110.13. 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).

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

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

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

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

112. As for **BCD**:

112.1. 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).

112.2. 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).

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

112.4. 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).

112.5. 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).

112.6. 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).

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

112.7.1. Carrying out information gathering exercises, including into:

112.7.1.1. The nature of the proposed recipient;

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

112.7.1.3. 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;

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

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

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

112.7.5. Ending sharing with a recipient if judged necessary;

112.7.6. 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.

112.8. 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.

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

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

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

114. In light of the above, the Claimant's submission that *"there 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, §96) is wrong.

115. It is also not accepted that the Respondents' position in respect of *"equivalence"* is unclear (contrary to Claimant's skeleton, §§96-98): see §110.9 and §112.8 above. More generally on this issue:

115.1. 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.

115.2. 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.

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

115.4. 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.

115.5. 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."*

116. 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.*"

117. The Claimant also asserts that there is *"little, if any"* Commissioner oversight over sharing of BCD/BPD (Claimant's skeleton, §86, §101). This is denied. The Intelligence Services Commissioner and Interception of Communications Commissioner have 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.[18] See also:

117.1. BPD: 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 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).

117.2. BCD: the Interception of Communications Commissioner has oversight over all aspects of disclosure of BCD (see Annex, §72).

117.3. In answer to a request by the Tribunal dated 13 April 2017 about what they regard as within their remit both Commissioners have 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"*.

118. The Claimants' submissions in this regard are simply unsustainable. There plainly is 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.

119. Finally, in relation to the Claimant's allegation that UK agencies, such as HMRC, are given access to bulk data (Claimant's skeleton, §§84(e), 94-95 and 104), this is not an

[18] Since 2010 in the case of BPD and since July 2015 in the case of BCD (October 2016 judgment, §§80-82) [**SA/2/24/§§80-82**].

issue which can be considered at the OPEN issues of law hearing in June 2017. The factual basis of the allegation is neither confirmed nor denied, and there is no agreed or assumed fact in relation to this (though CLOSED evidence addressing it has been filed). Accordingly, if it is considered necessary to determine this issue, it will be necessary to hold a CLOSED hearing to consider the evidence addressing it.

Industry partners

120. GCHQ shares operational data (which could in theory include BPD/BCD) 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.

EU law

121. The Claimant repeats (at skeleton §§103-105) its submission that BCD may not be transferred out of the EU, and that in relation to some of the data that may be held in BPDs, the safeguards identified in *Watson* must be adopted. The Respondents have already responded to those submissions at **Section D** above, and do not repeat their position.

G. Proportionality

122. 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.

123. As is made clear eg. in *Leander v Sweden* [**A/3/47**], 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/2/38**] at §§33-39).

124. 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. 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), and the increased difficulty in intercepting communications, make other capabilities, such as BCD and BPD, much more important to the SIAs.

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

125.1. 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).

125.2. 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.

126. 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.

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

127.1. 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;

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

127.3. 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.

128. 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.

129. 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.

130. The August 2016 *Report of the Bulk Powers Review* by David Anderson QC, the Independent Reviewer of Terrorism Legislation [**SA/2/27**], 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)

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

132. It is therefore submitted that the Respondents' s.94 BCD and BPD activities are proportionate and have been throughout each of the relevant periods.

133. The Claimant makes no separate submission concerning EU law as to proportionality, beyond its complaint that the safeguards identified in *Watson* in the context of DRIPA retention notices have not been adopted in the present context. That submission has already been addressed at **Section D** above.

JAMES EADIE QC

ANDREW O'CONNOR QC

GERRY FACENNA QC

ROBERT PALMER

RICHARD O'BRIEN

22 May 2017
Re-served with cross-references on 30 May 2017