

**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**

---

**SKELETON ARGUMENT  
ON BEHALF OF THE RESPONDENTS  
for hearing on 8-10 March 2017**

---

**A. Introduction and Summary**

1. The regimes applicable to the obtaining of BCD pursuant to a direction under s.94 of the Telecommunications Act 1984 (“**TA 1984**”) to a CSP, and to the obtaining of BPDs, by the UK Security and Intelligence Agencies (“**SIAs**”) pursuant to the Security Service Act 1989 (“**SSA 1989**”) and the Intelligence Services Act 1994 (“**ISA 1994**”) neither engage nor infringe EU law.
2. 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**”) 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*”) in the case of s.94 directions and Directive 95/46/EC (“*the Data Protection Directive*”) in the case of BPDs.
  - 2.2 that bulk retention of BCD and BPDs is unlawful under EU law;

- 2.3 that there is no mechanism to ensure that BCD acquired under s.94 and BPDs are used only for the purpose of fighting serious crime – and that is the sole purpose permitted under EU law; and
- 2.4 that the use of such BCD and BPDs lack safeguards which are mandatory under EU law, namely:
- (a) a requirement for independent authorisation for access;
  - (b) procedures for notification of use of the data;
  - (c) adequate controls on how they are shared; and
  - (d) 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. 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. The Claimant is also incorrect to suggest that EU law requires that BCD or BPDs may only be used for the purposes of fighting serious crime. That suggestion is based upon a misreading of *Watson*. See **Section D** below.
6. 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:
  - 6.1 In the context of national security, the effect of Article 4(2) TEU is that a Member State has 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.
  - 6.2 The safeguards identified in *Watson* were judged 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 they 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.
  - 6.3 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 E** below.

7. Finally, at **Section F** below, the Respondents deal with the proportionality arguments as now advanced by the Claimant, insofar as it is possible to do so in OPEN<sup>1</sup>. In summary, the Respondents' s.94 BCD and BPD activities are proportionate and have been throughout the relevant period:

7.1 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).

7.2 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.

7.3 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.

7.4 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.

7.5 **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.

---

<sup>1</sup> The Respondents' skeleton argument relating to the issues of the legality of sharing will be served by 4.00 pm on Friday 3 March, as ordered by the Tribunal at the interlocutory hearing on 1 March

- 7.6 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*”.
- 7.7 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.
- 7.8 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***

8. Article 4(1) and (2) TEU 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.*”

9. Article 5(1) and (2) TEU 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.*”

10. Notably, in the International Law Decision of 18-19 February 2016, 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.”*<sup>2</sup>

11. The effect of Article 4(2) was more recently explained in Case C-51/15 *Remondis*. 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:

11.1 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.

11.2 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.

12. 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.

13. Thus, when Article 16(2) TFEU 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*

---

<sup>2</sup> 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.

*regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.”*

14. Likewise, in Title V of Part Three of the TFEU (relating to the Area of Freedom, Security and Justice), it is confirmed that responsibility for national security remains with Member States, and is not conferred upon the EU. See:
  - 14.1 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
  - 14.2 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.”*
  - 14.3 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.”*
15. Consistently with Article 4(2) TEU and Article 16(2) TFEU, both the Data Protection Directive and the e-Privacy Directive exclude national security from their scope.
  - 15.1 Article 3(2) of the Data Protection Directive 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.”*<sup>3</sup>
  - 15.2 Article 1(3) of the e-Privacy Directive 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.”*<sup>4</sup>
16. Likewise, in the General Data Protection Regulation (Regulation (EU) 2016/679, which will repeal and replace the Data Protection Directive with effect from 25 May 2018, Recital (16) makes clear:

---

<sup>3</sup> See also Recital (13) of the Data Protection Directive.

<sup>4</sup> See also Recital (11) of the e-Privacy Directive.

*“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.”*

17. 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. In light of the primacy of Article 4(2) TEU and Article 16(2) TFEU, that was inevitable in the case of national security and essential State functions, given that competence in such matters had not been conferred upon the EU at all.

**(ii) Application to s.94 directions and BPDs**

18. 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.

19. 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.

20. In Joined Cases C-317/04 and C-318/04 *Parliament v Council* [2006] ECR I-4721, 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’ commercial purposes) to the United States authorities fell outside the scope of the Data Protection Directive. 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*, 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.

21. The Respondents’ response to this claim (as redacted and gisted for OPEN disclosure) confirms at §§7-16:

21.1 Both GCHQ and MI5 acquire BCD from providers of electronic communications services (referred to variously as “communications service 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.

- 21.2 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.
- 21.3 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.
- 21.4 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).
22. 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.
23. 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.
24. The recent opinion of AG Mengozzi in *Opinion 1/15* 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<sup>5</sup>. 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.
25. Since the purposes for which the data is processed fall outside the scope of EU law, Charter rights are not engaged:

---

<sup>5</sup> 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.

- 25.1 Article 6(1) TEU 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.*”
- 25.2 Moreover, Article 51(1) of the Charter 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***

26. 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.
27. In *Watson*, 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* at §43 and Case C-73/07 *Satakunnan Markkinapörssi* at §41. 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.*”
28. 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).
29. 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.

30. Against that background, the CJEU considered the effect of Article 15(1) of the e-Privacy Directive at §§71-74.
  - 30.1 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*”.
  - 30.2 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.
  - 30.3 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).
  - 30.4 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.
31. 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.

- 31.1 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.
- 31.2 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.
32. The Respondents emphasise that the context in which all of these observations are made concerns:
- 32.1 traffic and location data which is retained by *providers* (not State authorities);
- 32.2 access to such data which is provided by the further processing of the data by the *providers* (not State authorities); and
- 32.3 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)).
33. 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* 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 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.

34. 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* (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).
35. 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***

36. **First**, the Claimant contends (at skeleton §§21(c) and 41) that a s.94 direction is “*materially identical*” to a DRIPA retention notice. It is incorrect to do so. 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.
37. **Secondly**, the Claimant also seeks (at skeleton §§21(b) and 36-37) 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):

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

- 37.2 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 providers 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.
- 37.3 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.
38. **Thirdly**, the Claimant claims (at skeleton §26), without elaboration, that the obtaining of BPDs engages EU law pursuant to the Data Protection Directive. That is incorrect: 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).
39. **Fourthly**, the Tribunal is not assisted by the Claimant’s suggestion (at skeleton §§31-32) 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*.
40. **Fifthly**, the Claimant is also incorrect (at skeleton §§33-34) 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.
41. **Sixthly**, the Claimant contends (at skeleton §§35 and 39-40) 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 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 is otherwise ignored in the analysis, and plays no part in the *dispositif* – with good reason, as it falls out of scope. There is therefore no analysis at all of national security activities such as nuclear counter-proliferation, defence against cyber-attacks from 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).

42. **Seventhly**, the Claimant observes (at skeleton §42) 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) for use for other purposes, such as the detection of serious crime. However, the use 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.
43. **Eighthly**, the Claimant does not identify (at skeleton §44) any separate basis in EU law upon which it may be said that the BPD regime engages EU law. The correct position is that, for the reasons set out above, s.94 directions and the BPD regime do not fall within the scope of EU law.

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

44. The Claimant's bald assertion (at skeleton §22) 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:
  - 44.1 of a requirement on service providers
  - 44.2 for the general and indiscriminate retention of communications data
  - 44.3 which they would not otherwise have retained for any commercial or operational purpose
  - 44.4 for the purpose of fighting crime.

45. 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.
46. 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.
47. As to the **third**, just as under the s.94 regime, there is nothing in the BPD regime that requires any other individuals to retain any data either. Any data with which the BPD regime is concerned relates to data lawfully retained for the purposes of the activities of the data owners concerned.
48. As to the **fourth** of those points:
- 48.1 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.
- 48.2 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.
49. 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 purposes for which BCD and BPDs may be acquired or accessed are not limited to the purpose of fighting serious crime**

50. The Claimant contends 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. Even if and to the extent that EU law is engaged at all in the present context (which is denied), there would still not be any such requirement. The Claimant's contention to the contrary is based upon a misreading of *Watson*.

51. The starting-point (where they are engaged at all) is the terms of the Data Protection Directive and the e-Privacy Directive themselves. Neither restricts the purpose for which interference with any protected rights may be permitted to that of “*fighting serious crime*”.

51.1 Article 13(1) of the Data Protection Directive makes clear that

*“Member States may adopt legislative measures to restrict the scope of obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:*

- (a) national security;*
- (b) defence;*
- (c) public security;*
- (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;*
- (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;*
- (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);*
- (g) the protection of the data subject or of the rights and freedoms of others.”*

51.2 Article 15(1) of the e-Privacy Directive similarly makes clear that

*“Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3), (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of [the Data Protection Directive]. ...”*

- 51.3 In Case C-275/06 *Promusicae*, the court held at §53 that the express reference to Article 13(1) of the Data Protection Directive at the end of the list of exceptions in Article 15(1) of the e-Privacy Directive also authorised the Member States to adopt legislative measures to restrict the obligation of confidentiality of personal data (under Article 5(1) of the e-Privacy Directive) where that restriction is necessary for the purposes set out in Article 13(1) (including to protect the rights and freedoms of others).

52. Unsurprisingly, therefore, in *Watson* the CJEU held that a legislative measure which restricted rights under the e-Privacy Directive could be adopted to pursue any of those objectives (and confirmed its conclusion in *Promusicae* that the permitted objectives could include those set out in Article 13(1) of the Data Protection Directive), but no others: §§90, 115.
53. The CJEU then went on to hold that given the serious nature of the interference with rights under Article 7, 8 and 11 of the Charter, as a matter of proportionality, “*in the area of prevention, investigation, detection and prosecution of criminal offences*” (or “*fighting crime*” for short), only the objective of fighting “*serious*” crime was capable of justifying the legislative measures for retention and access to traffic and location data: §§102, 115. This was not a conclusion that the other objectives set out in Article 15 of the e-Privacy Directive could not justify a legislative measure interfering with such rights, as the Claimant contends. Instead, the CJEU concluded that where such legislation was sought to be justified by reference to the objective of fighting crime, the level of interference entailed would not be capable of being justified by reference to less serious crime (however that may be defined at a national level). That is why, in making such reference to a requirement that the interference be justified in the interests of “*fighting serious crime*”, the CJEU was careful to make clear that it was dealing with legislative requirements introduced “*for the purpose of fighting crime*”, or “*in the context of fighting crime*”: see §§102, 112, 115, 119 and 125. It is to be noted that the legislation at issue in the *Tele2 Sverige* case was expressly sought to be applied *only* in the context of fighting crime.
54. While the purposes for which retention notices could be issued or data accessed under the Data Retention and Investigatory Powers Act 2014 (“*DRIPA*”) were wider, in that they extended to any of the purposes set out in s.22(2) of the Regulation of Investigatory Powers Act 2000 (“*RIPA*”) (see §33), those purposes included that of “*preventing or detecting crime or of preventing disorder*”, without limitation as to the seriousness of crime or disorder involved: s.22(2)(b) RIPA. In that context, the CJEU chose to answer the first reference question in the DRIPA case together with the second question in the *Tele2 Sverige* case: see §§113-114, and to provide a single answer to it at §125. The result was that the court focused in particular on the particular question of the proportionality of providing access to retained data in relation to the objective of fighting crime, even though it recognised that other objectives were also permissible: §§115, 119.
55. The CJEU did not address the question of the proportionality of access to retained data in other circumstances:
- 55.1 Even where, at §119, the CJEU recognised that national security, defence or public security interests could be threatened, justifying greater access than it thought might otherwise be proportionate, it still did so in the context of “*particular situations*” including the prevention, investigation, detection or prosecution of specific cases of criminal (terrorist) activity.

- 55.2 It did not address the proportionality of access to retained data for other national security purposes, for example, in the context of the fight against nuclear proliferation, counter-espionage, defence against cyber-attacks by a foreign state, or military conflicts threatening the geo-political security of Member States of the EU (such as events in Ukraine or Syria). Still less, for the other legitimate objectives set out at Article 15(1) of the e-Privacy Directive and Article 13(1) of the Data Protection Directive.
56. The fact that the CJEU did not enter into a discussion of the proportionality of accessing retained data in such contexts cannot be taken to mean that the objectives set out in Article 15(1) of the e-Privacy Directive and Article 13(1) of the Data Protection Directive have been narrowed only to that of fighting serious crime. Such a contention is simply irreconcilable with both the CJEU's judgment, and indeed with the express terms of the legislation which the CJEU was seeking to interpret.

**E. 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**

57. 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:
- 57.1 a requirement for independent authorisation for access;
  - 57.2 procedures for notification of use of the data;
  - 57.3 adequate controls on how they are shared; and
  - 57.4 a prohibition on the transfer outside of the EU.
58. 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:
- 58.1 the proper approach to the assessment of proportionality and the breadth of discretion afforded to Member States on matters of national security;
  - 58.2 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*);
  - 58.3 the impact that that difference has on the appropriateness of and necessity for the safeguards identified in *Watson*.

59. 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***

60. The proportionality assessment is a fact-sensitive one, for the national court to apply. As it was put by Lord Reed and Lord Toulson JSC in *R (Lumsdon) v Legal Services Board* [2016] AC 697 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).”

61. 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.

62. 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, 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 for national security have particular wide discretion as to what is required.

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

63. 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.
64. **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.
65. **Second**, under the DRIPA regime (as under the Swedish laws discussed in *Tele2 Sverige*), 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:
  - 65.1 Compare the opinion of AG Mengozzi in *Opinion I/15* at §§178-179, relating to the draft agreement on the bulk generation of PNR data by air carriers flying between Canada and the EU: that act did not entail any interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter resulting from the EU’s draft agreement to provide that data to the Canadian authorities. See further *Watson* at §§86 and 92.

- 65.2 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.
66. **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).
67. **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:
- 67.1 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). In *Watson*, the CJEU was considering the requirements of necessity, appropriateness and proportionality for legislation falling within that derogation.
- 67.2 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*”. 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.

- 67.3 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).
- 67.4 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).
68. 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.
69. 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***
70. 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* at §§62-68 and *Schrems* at §95, which it considered applied by analogy in the context of the traffic and location data retention regimes at issue.
71. However, in *Opinion 1/15*, 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:
- 71.1 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.”*

71.2 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.”*

71.3 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.

72. 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.

73. 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.
74. 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 versions of the witness statements of each of the GCHQ, Security Service, and SIS witnesses. Save to note that they do not include the *Watson* requirements, the Claimant does not engage with that evidence. 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.

## **F. Proportionality**

75. 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.
76. As is made clear eg. in *Leander v Sweden*, 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* at §§33-39).
77. As explained in detail in the MI5 witness statement 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.

78. There is a clear value to **BCD** obtained by s.94 directions:
- 78.1 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, §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).
- 78.2 The MI5 statement 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.
79. 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.
80. **BPD** is a highly important capability for each of the SIAs. Examples of its usefulness are given at:
- 80.1 MI5 witness statement of 8 July 2016, §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;
- 80.2 GCHQ statement of 8 July 2016, §§16-18, §§106-114;
- 80.3 SIS statement of 8 July 2016, §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.

81. 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.
82. 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.
83. The August 2016 *Report of the Bulk Powers Review* by David Anderson QC, the Independent Reviewer of Terrorism Legislation, 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)*

84. The conclusion of the report was unequivocal: “*The operational case for [BPDs] is evident*” (§9.14(d)).
85. It is therefore submitted that the Respondents’ s.94 BCD and BPD activities are proportionate and have been throughout each of the relevant periods.
86. 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 E above.

**JAMES EADIE QC**

**ANDREW O’CONNOR QC**

**ROBERT PALMER**

**RICHARD O’BRIEN**

**2 March 2017**