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

B E T W E E N:

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

CLAIMANT'S SKELETON ARGUMENT
for hearing commencing 5 June 2017

References in the form ***[Bundle/Tab/Page]*** *are to the following bundles:*
- *Bundles used for the July 2016 hearing, namely "**Core"** and bundles numbered consecutively **1 to 5***
- *Supplemental bundle prepared for the hearing on 8 March 2017 ("**Supp1**")*
- *GCHQ exhibit bundle prepared for the hearing on 8 March 2017 ("**GCHQEx**")*
- *Second supplemental bundle, prepared for the directions hearing on 5 May 2017 ("**Supp2**")*

*If a further bundle is prepared for this hearing, it shall be referred to as the Third Supplemental Bundle ("**Supp3**").*

*The Authorities Bundles consist of five authorities bundles for the July 2016 hearing ("**A1**" to "**A4**" and a supplemental authorities bundle "**A5**") and a supplemental authorities bundle prepared for the hearing on 8 March 2017 ("**AS1**").*
*The further authorities bundle prepared for this hearing will be "**AS2**".*

I. INTRODUCTION

1. Following this Tribunal's earlier judgment ([2016] UKIPTrib 15_110-CH, [2016] HRLR 21 **[AS1/24]** (the '**October 2016 Judgment**')), three issues are to be determined at this hearing:
   a) the impact of EU law;
   b) the legality of transfer and sharing of data; and

c) proportionality.

Outstanding issues (including the report on searches, and issues 13 to 16 at **[Supp2/12/3-4]**) are to be determined at subsequent hearings.

2. In summary:

a) The collection of bulk communications data ('**BCD**') and bulk personal datasets ('**BPD**') engages EU law. The mandatory safeguards in Joined Cases C-203/15 and C-696/15 *Tele2 Sverige and Watson* ECLI:EU:C:2016:970 ('***Watson***') apply: blanket retention is prohibited, and there must be prior independent authorisation for access, notice provisions, retention in the EU and restrictions on the use of the material. Neither the regime under s.94 of the Telecommunications Act 1984 ('**TA 1984**') nor the BPD regime (so far as in scope) complies with the requirements of EU law. The Respondents' submissions to the alternative are untenable: the suggestion that the safeguards identified in *Watson* do not apply to processing for national security purposes is an argument already fought and lost by the Government. The suggestion that the IPT should ignore a decision of the CJEU is constitutionally unsound.

b) There appear to be no adequate safeguards governing the transfer of data from the Agencies to other bodies, whether they are other UK law enforcement agencies, commercial companies or foreign liaison partners.

c) The s.94 regime and the BPD regime are a disproportionate interference with Convention and EU Charter rights.

II. EU LAW

A. *Watson*

3. On 21 December 2016, the Grand Chamber of the Court of Justice handed down judgment in *Watson* **[AS1/17]**. The *dispositif* provides (underlining added):

> *"1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic*

communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

3. The second question [as to whether there is difference between EU and ECHR law] referred by the Court of Appeal (England & Wales) (Civil Division) is inadmissible".

4. The Grand Chamber affirmed its judgment in C-293/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 **[AS1/14]** and rejected the submissions made by the Secretary of State. The CJEU held that:

a) EU law is engaged by arrangements governing access to material retained by communications providers. The contrary arguments are dismissed (§71-73).

b) Blanket bulk retention of communications data is not lawful:

i) Directive 2002/58/EC (the '**e-Privacy Directive**') **[AS1/5]** seeks to ensure a high level of protection for communications, especially from automated storage and processing (§82-83).

ii) The e-Privacy Directive requires that systems be designed to limit data from ever being collected or retained, where possible (§87).

iii) Any derogation or exception must be strictly construed, otherwise the exception would become the rule and the protection given to the privacy of communications data by Article 5 of the Directive would become meaningless (§89, 103-104).

iv) The proper test is of strict necessity (§96).

v) The Swedish law provides for universal data retention (§97). It is therefore general and indiscriminate.

vi) Communications data is very sensitive and can be used for profiling. Universal collection leads to feelings of constant surveillance, which interferes with freedom of expression as well as the right of privacy (§99-101).

c) Retention of data is only proper for the purposes of preventing and detecting serious crime (including terrorism), given the seriousness of the interference with privacy involved in data retention (§115, 119).

d) There must be prior review of a request for access by a court or other independent authority, following a reasoned request, save in cases of urgency (§120).

e) There must be provisions for notification to persons whose data have been obtained, to enable their rights to be vindicated by complaint or legal proceedings, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities (§121).

f) Retained data must remain in the EU (§122).

5. All of the UK's submissions were rejected, including those as to the scope of EU law and whether EU law imposed mandatory requirements. The Grand Chamber confirmed its existing case law in *Digital Rights Ireland* (supra) **[AS1/14]** and C-362/14 *Schrems* ECLI:EU:C:2015:650 **[AS1/15]**, emphasising the importance of preventing blanket data retention and strong safeguards on access.

6. By a *corrigendum* dated 16 March 2017 (ECLI:EU:C:2017:222), the CJEU corrected the first sentence of one paragraph of the English and Swedish translations of its judgment in *Watson*. The first sentence of §111 previously provided:

> *As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to*

reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security.

The corrected version now provides, with amendments shown in mark-up:

As regards the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, ~~[and]~~ to contribute in one way or another to fighting serious crime or to prevent~~ing~~ a serious risk to public security.

The CJEU thereby clarified that its judgment was not merely about "*serious criminal offences*" but also dealt with processing of data to "*prevent a serious risk to public security*".

B. Legal framework

7. Article 7 of the Charter (which reflects Article 8 of the European Convention on Human Rights) provides **[AS1/3]**:

Everyone has the right to respect for his or her private and family life, home and communications.

8. Article 8 of the Charter provides **[AS1/3]**:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

9. Article 8(3) of the Charter has no direct analogue in the ECHR; there is no express right under the ECHR for all processing of personal data to be under the control of an independent authority. The official Explanations to the Charter[1] note **[AS1/25]**:

[1] The status of the Explanations is as follows: "*These explanations were originally prepared under the authority of the Praesidium of the Convention which drafted the Charter of Fundamental Rights of the European Union. They have been updated under the responsibility of the Praesidium of the European*

> *This Article [8] has been based on Article 286 of the Treaty establishing the European Community and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31) as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the Member States. Article 286 of the EC Treaty is now replaced by Article 16 of the Treaty on the Functioning of the European Union and Article 39 of the Treaty on European Union.*

10. Article 47 of the Charter, which harmonises the CJEU's case-law on effective remedial protection, provides (underlining added) **[AS1/3]**:

> *Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.*
>
> *Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.*

11. Article 51(1) of the Charter provides that it is "*addressed to… the Member States only when they are implementing Union law*" **[AS1/3]**.

12. Article 52(3) of the Charter provides **[AS1/3]**:

> *3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.*

Convention, in the light of the drafting adjustments made to the text of the Charter by that Convention (notably to Articles 51 and 52) and of further developments of Union law. Although they do not as such have the status of law, they are a valuable tool of interpretation intended to clarify the provisions of the Charter." Further, Article 6 TEU requires "*due regard*" to be given to the explanations, which set out the source of the provisions of the Charter.

13. Article 4 TEU provides **[AS1/1]**:

> *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.*
>
> *3. Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties.*
>
> *The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union.*
>
> *The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives.*

14. The e-Privacy Directive 2002/58/EC (the '**e-Privacy Directive'** or **'EPD**') **[AS1/5]** provides a harmonised level of protection across the Union for the confidentiality of communications and associated communications data. Article 1(2) states that its provisions particularise and complement the provisions of Directive 95/46/EC (the '**Data Protection Directive**' or '**DPD**' at **[AS1/4]**). Article 1(3) provides:

> *This Directive 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.*

15. Article 5 provides (underlining added):

> *1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). ...*

16. Article 6(1) provides that "*Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to … Article 15(1)*". Article 9 contains similar protections for location data.

17. Article 15 sets out the limits of any permissible derogation by a Member State:

> *1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6 … 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 Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.*

18. Article 22 of the Data Protection Directive provides **[AS1/4]**:

> *Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.*

19. The IPT is part of that framework of EU harmonised judicial remedies; the relief it offers must comply with Article 22 of the Data Protection Directive, and through it Article 47 of the Charter.

C. Application of *Watson* to BCD and BPD

(i) BCD Regime

20. A direction under s.94 TA 1984 to a communications service provider ('**CSP**') engages EU law:

a) Article 5 of the e-Privacy Directive requires that the confidentiality of telecommunications be ensured *except* when access is legally authorised in accordance with Article 15(1) of that Directive; likewise Article 6 of the e-Privacy Directive prevents all bar certain non-material forms of processing of communications data, unless authorised under Article 15(1).

b) The CJEU in *Watson* held that a retention notice issued under section 1 of the Data Retention and Investigatory Powers Act 2014 ('**DRIPA**') **[AS1/6]** fell within the scope of the e-Privacy Directive; see §§ 70-81 of *Watson*. At §73, the CJEU held **[AS1/17]**:

> *Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.*

c) A direction under s.94 TA 1984, imposing retention, processing and delivery requirements on a CSP in relation to BCD, is materially identical to a DRIPA retention notice for these purposes in that it requires the CSP to take actions that would otherwise be in breach of Articles 5 and 6 of the e-Privacy Directive. It therefore falls equally within the scope of the e-Privacy Directive.

21. Large-scale bulk retention of communications data is unlawful under EU law. See the summary of *Watson* at paragraph 4(b) above.

22. In any event, the statutory scheme under s.94 TA 1984 does not contain any of the necessary safeguards on access to data (see the summary of *Watson* at paragraphs 4(c) to (f) above). On its face, it permits interference with privacy and confidentiality rights that is unnecessary and disproportionate:

a) There is universal mass retention of communications data.

b) There is no requirement for prior independent authorisation for access.

c) There are no procedures for notification of use of the data.

d) There are no adequate controls on how BCD acquired under s.94 TA 1984 is shared.

e) Nor is there any prohibition on transfers of BCD outside of the EU.

23. The powers conferred by s.94 TA 1984 are entirely discretionary. There is no textual or interpretive barrier to reading s.94 as requiring the Secretary of State to exercise his discretion in accordance with the e-Privacy Directive. The Directive has been in force since 31 October 2003 and its material provisions are directly effective. Indeed, the relevance of EU law to s.94 TA 1984, even though it deals only with national security, is tacitly conceded by the introduction of proportionality as the controlling concept in s.94(2A), a change made by the Communications Act 2003 (the Act which transposed all of the CRF Directives).[2]

24. None of the section 94 Directions disclosed to date contain *any*, still less *all* of the mandatory safeguards required by *Watson*. It therefore follows that all such directions are *ultra vires* and have been since 31 October 2003. As such, since that date all action taken pursuant to such directions is not "*in accordance with law*" and necessarily breaches Articles 7 and 8 of the Charter.

25. Further, and in any event, the section 94 regime is unlawful for the same reasons as previously advanced in relation to the ECHR. The section 94 regime is not prescribed by law and is a disproportionate interference with fundamental rights.

(ii) BPD Regime

26. The obtaining of BPDs engages EU law pursuant to the Data Protection Directive **[AS1/4]** (see further paragraph 46 below).

27. Where the information contained in a BPD is of a broadly equivalent level of intrusiveness to communications data, the principles of necessity and proportionality will require an equivalent level of safeguards governing access to data as those

[2] See Schedule 17 to the Communications Act 2003, paragraph 70 **[A1/8/815]**.

identified in *Watson*. See the Opinion of Advocate General Mengozzi in *Opinion 1/15* ECLI:EU:C:2016:656 (8 September 2016) concerning the EU-Canada draft agreement on the transfer and processing of Passenger Name Record Data (in particular, §§169-171, 328) **[AS1/18]**.

28. Such datasets are likely to include:

a) BPDs containing intercept material (it has been avowed that "*some BPDs are obtained by interception*" – David Anderson QC *Bulk Powers Review* (August 2016), footnote 119 **[AS1/27/48]**).

b) health datasets (the Agencies have said that they do not currently retain such datasets, although they presumably might do so in the future, and may have done so in the past);

c) financial datasets (e.g. information about personal expenditure, which will often include location);

d) location and travel datasets (e.g. Automatic Number Plate Recognition and Oyster card data); and

e) any BPDs containing privileged material or identifying journalistic sources.

29. The BPD regime does not contain any of the safeguards referred to above; it therefore permits interference with privacy and confidentiality rights that is unnecessary and disproportionate:

a) There is mass retention of BPD.

b) There is no requirement for prior independent authorisation for access.

c) There are no procedures for notification of use of the data.

d) There are no adequate controls on how BPDs are acquired are shared.

e) Nor is there any prohibition on transfers of BPDs outside of the EU.

D. Respondents' submissions

30. The Respondents make four points in their Outline Response of 10 May 2017:

a) On a proper reading, the CJEU confined its judgment in *Watson* to retention of and/or access to data for the purposes of the investigation, detection and prosecution of serious crime, and not in respect of national security, because such matters are outside the scope of EU law pursuant to Article 4(2) TEU.

b) Alternatively, if the Data Protection Directive and/or e-Privacy Directive were engaged by section 94 Directions, *Watson* should be distinguished on the basis that a different proportionality balance may be struck in respect of such processing in the interests of national security.

c) Alternatively to (a) and (b), if the CJEU's judgment purported to make findings in relation to the retention of and/or access to databases for the purposes of national security, the judgment should be read down to avoid that conclusion.

d) As a further alternative argument (which it is not yet confirmed whether the Respondents will pursue, but which is addressed below), the Tribunal is not bound by the CJEU's judgment, because the CJEU does not have competence to make a binding determination as to the proper interpretation of the TEU

31. None of these points has any merit.

(i) The *acquis communautaire*, national/public security and the scope of EU law

32. Community/EU law has long had to grapple with issues of national security, well before what is now Article 4(2) TEU was incorporated (by the Treaty of Amsterdam) or became justiciable by the CJEU (by the Treaty of Lisbon). The *acquis communitaire* settled before this date (and the basis on which Article 4(2) TEU was agreed by the Member States) shows that national security *per se* is not wholly outside the scope of EU law. This is self-evident from the fact that repeatedly the TFEU itself provides for national/public security to be either a ground of derogation from Treaty rights, notably the "Four Freedoms" (see below), or a source of special TFEU rules (as with 346 TFEU, relating to the arms trade).

33. Rather, what the consistent case-law of the CJEU, applied time and again by both it and national courts (including English courts) shows, is that where national security is relied upon as a reason to curtail, restrict or interfere with a right, liberty or harmonised obligation provided or safeguarded by EU law, such topic *is* in scope of EU law.[3]

34. To give but the simplest example, where X, a citizen of Member State A, wishes to travel to Member State B to take up a job (thereby exercising her right of free movement), and Member State B wishes to exclude X from B on grounds of national security (A is assessed to be a potential dangerous radicalising influence), the resulting dispute *is* within the scope of EU law. It is no answer for the Member State to say that it excluded X on grounds of national security, such that Article 4(2) TEU means that the matter is outside the scope of EU law and any CJEU decision should be ignored as *ultra vires*.

a) The first and most obvious reflection of this is the fact that the relevant rights of free movement for workers and the self-employed are subject to express public security exceptions: see e.g. Article 45(3) TFEU. Public security has long been understood and held to embrace (as a sub-category) national security. Thus, national security is both in scope and amenable to control through EU general administrative principles (EU human rights, proportionality etc.). In the field of free movement of people, such has been the consistent position of the CJEU ever since the seminal 1974 case of *Van Duyn* [1974] ECR 1337. See for a recent statement of this principle Case C-430/10 *Gaydarov* ECLI:EU:C:2011:749 at [32].

b) Indeed, it was the engagement of EU law, and its stricter requirements for a fair hearing even in an immigration context (i.e. one which would be outside Article 6 ECHR), in an unequivocal national security context that provided (along with the ECHR case-law) one of the two reasons for the creation of SIAC, following the CJEU case of *Gallagher*[4] (in which a known IRA member was expelled from

---

3 Steve Peers 'National Security and European Law', *Yearbook of European Law*, 16 (1998), pp. 363-404.

4 *R v Secretary of State for the Home Dept, ex p Gallagher* (Case C –175/94) [1995] ECR I–4253. See also Joined Cases C-65/95 and C-111/95 *R (Mann Singh Shingara and Abbas Radiom) v Secretary of State for the Home Department* [1997] ECR I-3343.

the UK on the basis of his 'implication in', rather than commission of, terrorist acts), itself building on C-222/84 *Johnston v RUC* [1986] ECR 1651 (another case with a clear national security context), and the clear indication contained therein that the appeals regime then in force for national security based expulsions did not comply with EU law. The SIAC Act 1997 was passed. The first case testing the new regime was a further EU case, *Loutchansky*, involving the exclusion of a key officer of an EU company (Nordex) on national/public security grounds.[5]

c) It is for this very reason that the key pieces of EU secondary legislation dealing with free movement rights, such as the Citizenship Directive (2004/38/EC), contain provisions dealing with public/national security exclusions: see its Recitals 16, 22-24, Article 1(c), 15(1) and Chapter VI. These provisions both recognise a national security exemption/derogation, *and* control the exercise of national security decision making by Member States by subjecting such decisions to scrutiny by EU administrative law principles. The most recent example is the important CJEU judgment involving the UK in Case C-300/11 *ZZ* ECLI: EU:C:2013:363 **[AS1/13]**. *ZZ* was a pure national security case originating in SIAC, which called for detailed consideration of the above cited provisions of the Citizenship Directive; see also [63]-[75] of the AG's Opinion, where AG Bot found the national security exemptions in the legislation to be within the scope of EU law, leading to the application of the Charter, including consideration of Article 4(2) TEU (ECLI:EU:C:2012:563).[6]

d) Similar provisions appear in the key asylum Directives: see Case C-601/15 PPU *JN* ECLI:EU:C:2016:84 for a recent public/national security case of exactly this type.

e) Equally a similar approach is applied when dealing with restrictions (whether substantive or procedural) in employment claims governed by EU law, such as race or sex discrimination claims: see *Kiani v SSHD* [2016] QB 595 in which there

---

5 The SIAC strike out application in *Loutchansky* cannot be located; but a flavour of the litigation can be obtained from the subsequent judicial review brought to recover costs: *Loutchansky v First Secretary of State* [2005] EWHC 1779 (Admin).

6 Case C-300/11 *ZZ v SSHD* [2013] QB 1136 **[AS1/13]**.

was no dispute but that EU law applied to a race discrimination claim, the focus of enquiry being *inter alia* the demands of EU law with respect to gisting in a closed material procedure.

35. The corollary of this principle, and the true import of Article 4(2) TEU is that:

a) the activities of the security services of Member States *are* outside the scope of the TFEU insofar as they do not disturb the rights and obligations imposed by EU law. So, to give an example, the monitoring or surveillance of an EU national by conventional means (e.g. a Covert Human Intelligence Source or surveillance team) is outside the scope of EU law, whereas the act of seeking expulsion/exclusion based on the product of such surveillance is not; and

b) the EU has no competence to undertake work to further the national security of any Member State. So it cannot comment on the adequacy of any state's efforts or demand particular steps be taken; nor set up its own intelligence agencies.

36. Precisely the same analysis applies in relation to both the Data Protection Directive and the e-Privacy Directive. Both instruments were intended to complete the internal market, by harmonising the standards with which EU businesses would have to comply across the EU: see e.g. Recital (7) DPD **[AS1/4]**. The effect of the e-Privacy Directive is to provide assurance to, say, a German law firm considering buying telecoms services from a UK company (e.g. Vodafone) as to the standards of confidentiality, privacy and protection of data that it can expect. By providing common standards across the EU, competition across the internal market is promoted. The harmonising impetus of the e-Privacy Directive, part of the so-called Common Regulatory Framework ('**CRF**') for telecommunications along with the Framework Directive (2002/21/EC), the Access Directive (2002/19/EC), the Authorisation Directive (2002/20/EC) and the Universal Service Directive (2002/22/EC), is, if anything clearer still. The CRF in general, and the EPD in particular, was designed to complete the internal market in the provision/receipt of telecommunications services: see Recital 3 of the old Privacy Directive (97/66/EC) and Recitals (4) to (8) of the EPD replacing it. The foundational principle of the e-Privacy Directive is that (for privacy/fundamental rights reasons) only certain very limited

forms of processing of either communications or communications data should be permitted.

37. It is in this context that Articles 1(3), 6 and 15 EPD fall to be understood **[AS1/5]**:

a) Article 1(3) says the Directive shall not apply to activities "*concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters)*". That is because these activities fall outside the scope of the treaties. The exception in Article 1(3) would encompass e.g. non-commercial telecommunications activities or services of the defence or security services (such as MOD phone or secure mobile, radio etc.).

b) Article 5 guarantees the confidentiality of both communications and communications data by imposing strict confidentiality obligations on any public communications network ('**PCN**') and any publicly available electronic communications service ('**PECS**')and provides that such material can only be accessed by third parties with a legal authorisation (a warrant etc.) granted under Article 15.

c) Article 6 then imposes an obligation on PCNs and PECSs to erase all communications data, subject to very limited exceptions. This is a harmonised obligation imposed on PCN/PECSs designed to provide a level regulatory playing field, so that service provider A can provide communications services to X in country B without adapting its platform or offering. It also provides a guarantee as to common privacy standards to customers across the EU, thus encouraging use of foreign providers and competition.

d) It is thus (like a number of other provisions in the EPD) an obligation whose real function is, through harmonisation of obligation, to further or give real effect to the PCN/PECS's right freely to provide services across borders and/or to establish itself or branches in other Member States, pursuant to establishment rights in Article 49 TFEU (subject to the public security derogation in Article 52.1) or service provision rights in Article 56 TFEU (subject to the public security derogation in Article 62).

e) Article 15 then qualifies that obligation of privacy and data erasure by stating (emphasis added):

> *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) and (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 Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.*

38. Seen for what it is, such regime conforms in all material ways with that applied to the exclusion of persons from a Member State. EU law confers rights and corollary harmonised obligations, both under the Treaty and more relevantly under secondary legislation. If national security is relied upon as a basis for derogating from that harmonised scheme, then such derogation is within scope of EU law, just as much as the decision to expel or deny entry to a suspected terrorist of EU nationality.

39. The basis for engagement of EU law in *Watson* was simple: DRIPA purported to impose very substantial obligations of processing and cost upon PCNs/PECSs. DRIPA therefore engaged EU law because it rewrote the Article 6 retention obligations (as Article 15 permitted)[7] and as such would have a hugely market partitioning effect if each of the 28 EU Member States imposed their own data retention rules requiring data. A PCN/PECS wishing to provide services throughout the EU would then have to comply with up to 28 different sets of legal standards, potentially conflicting in nature (e.g. if States A and B operated different mandatory deletion rules that would create a conflict in relation to

[7] Even were there no EPD because, for the sake of argument, it were *ultra vires*, such an obligation would engage general Treaty rights because it would be a clear restriction engaging the C-55/94 *Gebhard* [1995] ECR I-4165 test; the fact that any new entrant to the UK PCN market would have to build/provide systems ensuring compliance with a probable section 94 Direction is a substantial barrier to entry.

calls between those two states). Such a state of affairs would be and is obviously a serious impediment to providing telecoms services throughout the single market.

40. It is common ground that a section 94 Direction involves processing of communications data by the PCN/PECS. The Respondents have made a belated but substantial concession (as they did at the Directions Hearing on 5 May 2017, repeated in the Outline Response of 10 May 2017) that a section 94 Direction requires processing just as a DRIPA retention notice did. This engages the rights and harmonised obligations in the e-Privacy Directive (in this case both Article 5 and Article 6(5)). In these circumstances, the case that EU law is engaged with respect to BCD is unanswerable.

41. Accordingly, s.94 TA 1984 can be used to obtain BCD only in conformity with Article 15 EPD; and thus with the EU fundamental rights and EU Charter scrutiny that goes with it.

42. There is nothing revolutionary or new in such analysis. Indeed, it is precisely the analysis of both the Chancery Division and Court of Appeal in the Floe Telecom litigation, culminating in *Recall Support Services Ltd v Secretary of State for Culture Media and Sport* [2014] EWCA Civ 1370.

    a) In that case, Ofcom had placed restrictions on the commercial use of commercial multi-user and single user GSM gateways ('**COMUGS**' and '**COSUGs**'). These types of telecommunications switching equipment could be legitimately used to place cheaper mobile telephone calls. But communications data relating to the call may be obfuscated as a result of the call passing through the switching equipment. The restrictions therefore had a national security rationale.

    b) At the heart of the litigation was the contention that the restriction was justified by national security considerations (although unexplained in the judgment, the obvious concern was that calls made through such a GSM gateway would be hard to trace and so would impede the efficacy of section 94 Directions or other interceptions).

c) The judge held that the national security case failed for COSUGs but not COMUGs, but that there was no "sufficiently serious" breach for EU state liability, a conclusion upheld on appeal. At no stage, whether before Rose J [2013] EWHC 3091 (Ch) or on appeal (in which the Home Secretary was represented by Mr Beard QC throughout, who also represented the UK in *Watson*), was it suggested that such a restriction – a ban on the use of telecoms equipment in the interests of national security – took the claim wholly outside the scope of EU law, an argument which would have defeated the claim *in limine*.

43. The Respondents' argument that *Watson* does not apply to action taken for national security reasons is also in substance a collateral attack upon the validity of a judgment to which the Secretary of State was a party where the arguments it seeks to put about Article 4(2) TEU and Article 1(3) of the EPD were made, heard and rejected:

a) In *Watson* before the domestic courts, the Respondents conceded that EU law was engaged by a DRIPA retention notice. However, by the time of the reference, the Respondents had withdrawn their concession and expressly sought to rely on both Article 4(2) TEU and Article 1(3) of the e-Privacy Directive: see *Watson* at §65 **[AS1/17]**; and see, more fully, §20-30 of the UK's observations in *Tele2 Sverige* **[AS1/29/8-12]** and §18-19 of its observations in *Watson* **[AS1/30/7-8]**. A note of the submissions made by the UK during the oral hearing in *Watson*[8] records HM Government making the following submissions:[9]

> *What is more important is Art 1(3) is v. careful to limit the directive's scope and what is outside the scope of EU law. That is something that we need to have*

[8] The CJEU has been asked to grant the Claimant access to the recording of the hearing, in order to produce a verbatim transcript. The Respondents have been provided with a copy of the note taken during submissions and invited to provide their comments on its accuracy.

[9] As this note records, the Government sought to rely on the extract of the conclusions of the European Council of 18-19 February 2016 "A new settlement for the United Kingdom within the European Union" **[AS1/31]**. The Respondents are again seeking to rely on this document in these proceedings. However, it is without legal effect, given the UK's decision to leave the EU. As the document recognises, it sets out arrangements which "*will become effective on the date the Government of the United Kingdom informs the Secretary-General of the Council that the United Kingdom has decided to remain a member of the European Union*" (§2). Needless to say, that condition precedent was not met. The UK's Article 50 TEU notice was served on 29 March 2017. Pursuant to Article 50(3) and the European Communities Act 1972, EU law remains in effect.

carefully in mind. Also, the member states have set out carefully in Art 4(2) TEU, and Protocols 21 & 22 of the treaties. And affirmed this February by Heads of State. They have confirmed that national security remains the preserve of the Member States. Why matter here? CJEU couldn't be laying down rules about matters outside EU law, nor matters outside [EPD]. *That would only be singling out a part of access arrangements. This would be surprising. We say it would be wrong. We concur with CA in UK that* [the judgment in *Digital Rights Ireland*] *was simply absence of any standards at all. It is a proportionality review.*

b) The UK Government made these submissions because it well understood that DRIPA *was* national security legislation. The suggestion that DRIPA and *Watson* were about criminal investigation alone is wrong. DRIPA expressly permits a retention order to be made for the purposes of national security.[10] It is to be assumed that DRIPA retention orders have been made for national security purposes. The CJEU was well aware of the use of DRIPA for national security purposes.[11]

c) The UK Government's arguments about the scope of EU law were rejected by the CJEU. In a detailed judgment, the CJEU referred to the various submissions made about the scope of EU law (*Watson* at §§65-66). The Court then cited Article 1(3) and noted that it overlapped with Article 15(1), and referred to the national security context (at §72).

d) The CJEU then held (in line with *Digital Rights Ireland*) that a national data retention measure was within the scope of EU law, both as regards retention and as regards access to that data retained by the service provider: see *Watson* at §§73-81, especially §§75-76 and §78 (in which the CJEU refers to granting access to data "*for the purposes set out in [Article 15(1)]*"). The reasoning necessarily applies to all the purposes listed in Article 15(1) of the e-Privacy Directive, including national security.

---

10 Section 1(1) of DRIPA provided **[AS1/6]**: "*The Secretary of State may by notice (a "retention notice") require a public telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000 (purposes for which communications data may be obtained).*" Section 22(2)(a) of the Regulation of Investigatory Powers Act 2000 ('**RIPA**') identifies a purpose as "*in the interests of national security*" **[A1/7]**.

11 The above domestic statutory regime was set out by the CJEU in *Watson* at §§29 and 33 **[AS1/17]**.

e) Further, in subsequent passages after the scope issue was decided, the CJEU expressly held that its ruling applied to data retention for the purposes of national security. Notably, the Court indicated the (limited) extent to which the mandatory requirements it identified were to be applied differently in national security cases (at §§ 90 and 119, emphasis added):

> *It must, in that regard, be observed that the first sentence of Article 15(1) of Directive 2002/58 provides that the objectives pursued by the legislative measures that it covers, which derogate from the principle of confidentiality of communications and related traffic data, must be 'to safeguard national security – that is, State security – defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system', or one of the other objectives specified in Article 13(1) of Directive 95/46, to which the first sentence of Article 15(1) of Directive 2002/58 refers …*
>
> *… access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime … . However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.*

f) The Court thus tailored its judgment to national security cases. The adjustments made to its approach in national security cases is fatal to the Respondents' argument that national security retention was not being considered in *Watson*.

44. The critical point is thus this: it is the fact that it is the effect of a section 94 Direction to rewrite EU law and obligations of UK PCN/PECSs (as a permissible derogation envisaged by EU law) and the burden such directions impose on UK PCNs, notwithstanding the close harmonisation effected by the EPD, that brings the dispute within scope of EU law.

45. Nothing in Article 4(2) TEU alters that analysis. When the Agencies mandatorily co-opt private actors to undertake or contribute to their surveillance/data-gathering activities, such activities do engage EU law. Free-standing activities (e.g. interception of communications without compulsion or assistance from a PCN/S) do not engage EU law. But those are not the activities considered here.

46. Similarly, in respect of BPDs, the engagement of EU law is a function of the type of database and how it was acquired from the private party who originated it. Where the Agencies mandatorily co-opt private commercial actors, particularly those working in a field engaging free movement rights, to provide such a database, EU law is engaged, whether through the Data Protection Directive or through general EU law principles. For example, if the Secretary of State issued a direction to an airport operator (a classic cross-border service provider) under s. 30 of the Airports Act 1986[12] to assemble and/or hand over a database, the burden imposed on that private party will be a relevant restriction within the meaning of the DPD.

(ii) <u>The Respondents' '*kompetenz-kompetenz*' arguments</u>

47. There are two basic problems with the Respondents' case on *kompetenz-kompetenz*, as now advanced after prompting from the Tribunal.

48. The first problem is that even the cases tentatively identifying the possibility in English law of control over the EU/CJEU's assumption of powers do so only where such control can be exerted by reference either to: (i) a clearly definable domestic constitutional principle that itself operates to qualify ordinary statutory construction; or (ii) a clearly defined reservation of national legislative and judicial competence (a so-called *renvoi* to national law) negotiated and incorporated as part of the Treaty conferring additional powers on the EU polity. There is no such 'hook' in the present case for the assertion of a national court competence to review the jurisdictional boundaries of a CJEU decision, not least since Article 4(2) TEU plainly does not operate to take rights/obligations conferred by EU law out of the scope of the Treaties.

49. The second problem is that the Respondents' case on remedies is incoherent: the putative distinction between a doctrine of interpretation to avoid constitutional conflict and a *'kompetenz-kompetenz'* argument (which still awaits potential approval) does not

---

12 Section 30(1) of the Airports Act 1986 provides: "*The Secretary of State may give to any airport operator or to airport operators generally such directions of a general character as appear to the Secretary of State to be necessary or expedient in the interests of national security or of relations with a country or territory outside the United Kingdom.*"

work, since both approaches are predicated upon a prior decision by the national court that but for the remedy, enforcement of the EU judgment would violate a superior domestic constitutional norm or protected area of national competence. Moreover, the interpretative remedy is unworkable on the facts (and a long way from its original moorings in the German BvfG decision in its Counter-Terrorism Database Act decision).

50. The true position is that this entire line of argument (which originated with the Tribunal itself, and formed no part of the Government's original skeleton argument) would not have surfaced at all had the UK merely won or lost on the previously anticipated lines of battle from *Watson*, namely whether or not prior judicial authorisation was required for access. The reality is that UK Government and UK courts have long accepted that EU law imposes limitations on the actions it may take in the name of national security to qualify, derogate or restrict rights and/or the harmonised regime provided and protected by EU law (as the insertion of s.94(2A) TA 1984 itself shows); all that is really different about *Watson* is the degree of control exerted is greater than HM Government wants, despite having had the two opportunities to persuade the CJEU to the contrary in *Digital Rights Ireland* (as an intervener) and in *Watson* (as a full party). The only legitimate remedy might lie in inviting the IPT, as a final Court under Article 267(3) TFEU, to refer further questions to the CJEU to clarify the supposedly differential application of *Watson* in a pure or primarily national security case or ask for confirmation that it applies to a power like s.94 TA 1984. Even that course is unnecessary because the answer is plain.

(a) No scope for the application of a UK kompetenz-kompetenz doctrine in the present case

51. It is important to note that the Respondents' *kompetenz-kompetenz* case raises and, at §6 of the Amended Respondent's Outline Response Document, conflates two logically separate, if related issues. Those are:

a) which Court interprets the Treaties and the various pieces of secondary legislation made under them (the **"Interpretation Task**"); and

b) which Court determines whether the Treaties and secondary legislation, so interpreted, respect the boundaries of the powers conferred on the EU

institutions by the underlying Member States i.e. which court has ultimate say on jurisdictional boundaries, or *kompetenz-kompetenz*.

52. All of the national higher court case-law throughout the EU, including that addressing *kompetenz-kompetenz*, takes as read that the CJEU undertakes the Interpretation Task. So far as the Applicants are aware, neither the UK Supreme Court, the German BvfG, the French Conseil Constitutionel, nor any substantially reasoned judgment of any English Court (whether *Pham* or *HS2* – discussed below) has suggested that the initial Interpretation Task is other than for the CJEU. The reasons are obvious: first, that is the very rationale for the existence of the CJEU – a specialist Court with linguistic and EU law expertise whose function is to interpret EU law; second, any other course is a recipe for the Treaties and the instruments made under them to have different interpretation and (in the case of secondary legislation) variable validity throughout the EU: in short legal anarchy. It would be impossible to operate a single market if EU legislation were given a different meaning in different EU Member States. Any assertion of *kompetenz-kompetenz* must therefore be truly exceptional and confined to the narrowest of cases if it is not to constitute an existential threat to the integrity of the EU legal order.

53. Indeed, it is the very fact that the CJEU has been entrusted with the Interpretation Task, along with the inference from it that EU law is intended to have a consistent and uniform effect throughout the contracting states, that has provided much of the impetus for the seminal planks of the CJEU's constitutional jurisprudence, in cases as diverse as:

a) *Van Gend en Loos* [1963] ECR 1 (direct effect);

b) *Costa v ENEL* [1964] ECR 585 (supremacy);

c) *Da Costa* [1963] ECR 31 (precedential effect of clear ruling);

d) *Simmenthal* [1978] ECR 629 (supremacy, even with respect to subsequent national laws);

e) *CILFIT* [1982] ECR 3415 (uniformity of interpretation as the goal of preliminary rulings);

f) *FotoFrost* [1987] ECR 4199 (the CJEU's monopoly over ruling on the validity of EU secondary legislation); and

g) *Marleasing* [1990] ECR I-4135 (conforming interpretation).

54. Such doctrines have long been uncritically received into English law, both through the European Communities Act 1972 ('**ECA 1972**') (which, in effect, enacts the supremacy of EU law) and subsequent domestic case law, including *R v Secretary of State for Transport, ex p. Factortame Ltd* (No.2) [1991] 1 AC 603. But, most critically, any suggestion that the UK national courts have any *superior* (or oversight) role in relation to the Interpretation Task is impossible to reconcile with Parliament's instruction to the Courts in s.3(1) ECA 1972, which is expressed in plain and unambiguous terms as follows:

> *For the purposes of all legal proceedings any question as to the meaning or effect of any of the Treaties, or as to the validity, meaning or effect of any EU instrument, shall be treated as a question of law (and, if not referred to the European Court, be for determination as such in accordance with the principles laid down by and any relevant decision of the European Court).*

55. Section 3(1) says, and decided cases take it to say, that decisions of the CJEU are binding: see e.g. *Factortame No.*2 at 658-9, and 660B per Lord Bridge; *Miller v Secretary of State for Exiting the European Union* (DC) [2016] EWHC 2768 (Admin) at [54] and [93(7)]; and *Dawson v Thompson Airways* [2014] EWCA Civ 845 at [22]-[24] per Moore-Bick J (in the context of the effect of the controversial CJEU *Sturgeon* ruling, held to be binding).

56. In the light of s.3(1) ECA 1972 there is no room for argument as to two propositions (which dispose of the Interpretation Task):

a) national Courts must determine cases turning on questions of interpretation of EU Treaties and instruments in line with the principles identified by the CJEU; and

b) CJEU decisions sit at the apex of the English doctrine of precedent, such that the national court's only option (if unconvinced by an earlier ruling in a related matter) is to refer questions to the CJEU.

57. Once the meaning of the relevant Treaty or secondary instrument has been identified by the CJEU, a distinct question may arise: is the CJEU ruling and the state of EU law identified therein consistent with the limited powers *conferred* on the EU by the underlying Member States and/or with the way that national implementation of EU obligations has been or will be undertaken? This problem has been most extensively considered in those states (most obviously Germany) with a developed and entrenched written constitution, containing clear and express allocations of power and competence, which thus set domestic limits upon international treaty negotiation and the cession of power by a national Parliament.[13] Moreover, such *kompetenz-kompetenz* issues predominantly arise at the stage of power *conferral* where national constitutional courts exercise a form of *ex ante* control to test whether the proposed conferral of additional powers on the EU (e.g. by the Maastricht or Lisbon Treaty)[14] is consistent with the national constitution. Far less common is *ex post* review (or more accurately the *threat* of it), though this was the origin of the BvfG's famous *Internationale Handelsgesellshaft mbH/"Solange"* case-law (on fundamental rights protected by the Grundgesetz)[15], that led the CJEU to develop its own autonomous EU fundamental rights (that ultimately led to the Charter)[16] and of the only extant instance of actual refusal to apply a CJEU ruling on domestic constitutional *ultra vires* grounds.[17]

---

13 A good historical and comparative account of *kompetenz-kompetenz* can be found in P Craig, "*The ECJ, National Courts and the Supremacy of Community Law*", at http://www.ecln.net/elements/conferences/bookrome/craig.pdf; and in T. Tridimas' contribution in Ch.16 of the Oxford Handbook of European Union Law, "*The ECJ and the National Courts: Dialogue, Cooperation, and Instability*" (OUP, 2015). See also See Gunnar Beck, '*The Problem of Kompetenz-Kompetenz: A Conflict between Right and Right in Which There Is No Praetor*', European Law Review 30 (2005) 42ff.

14 See respectively the BvfG Decisions in: BverfGE 89, 155, reported in English as *Brunner v European Union Treaty* [1994] 1 CMLR 57 (Maastricht); and BverfGE 123, 267, reported in English as *Re Ratification of the Treaty of Lisbon* [2010] 3CMLR 13 (Lisbon).

15 *Internationale Handelsgesellschaft* (1974) BverfGE 37, 271; reported in English at [1974] 2 CMLR 540

16 See Craig, *Ioc cit* pp.39-40.

17 See *Landtova*, as discussed in R. Zbiral 'Czech Constitutional Court, Judgement of 31 January 2012, Pl US 5/12, A Legal Revolution or a Negligible Episode? Court of Justice Decision Proclaimed Ultra Vires' [2012] CMLRev 1475. The point was a very narrow one relating to Czech constitutional provisions seeking to maintain equal treatment in pension entitlements of Czech and Slovak nationals after the dissolution of Czechoslovakia. Tridimas, *loc cit*, states at p.421 that "*Defiant as it was, the judgment did not raise strategic issues of European integration*."

58. Until very recently there has been little trace in English case law even of potential interest in participation in the form of 'Apex Court Dialogue' such constitutional doctrine tends to produce. The reason is clear: the cardinal, organising UK constitutional principle is that of Parliamentary sovereignty. Once Parliament has transplanted EU law, as amended from time to time by the EU institutions, and as interpreted by the CJEU, in its entirety into the UK legal order, and instructed the Courts to follow CJEU case law and to treat it as binding, there is, at first sight, no other superior constitutional principle around which to structure an argument contending, in effect "*but that power could not lawfully be conferred on the CJEU*".

59. Two recent cases (or lines of case-law) suggest the Supreme Court may be willing to countenance a *kompetenz-kompetenz* argument in very limited circumstances: *HS2* and *Pham*.

60. *R (on the application of Buckinghamshire CC) v Secretary of State for Transport* [2014] UKSC 3, [2014] 1 WLR 324 ("***HS2***") concerned a challenge to the legality of the use of the Hybrid Bill procedure to pass a Private Act of Parliament authorising the HS2 line. The claimants contended that whilst the relevant EU law permitted a legislative process to be used, that was lawful only when criteria set by the CJEU as to the quality of the legislative process (in terms of consultation, engagement with issues etc.) were met; and it could not be said the Hybrid Bill procedure would meet such: see [67]-[76] per Lord Reed for a summary of the arguments.

    a) Lord Reed identified that such arguments, if right, would offend against the constitutional principle of long-standing, embedded in Article 9 of the Bill of Rights, that courts cannot enquire into or pass comment or judgment upon Parliament's process, noting at [78] that "*it follows that the claimants' contentions potentially raise a question as to the extent, if any, to which these principles may have been implicitly qualified or abrogated by the European Communities Act 1972*." As will be appreciated, *HS2* raised a significant point of UK constitutional importance. When two 'constitutional' statutes (the ECA 1972 and the Bill of Rights) may be inconsistent, how is the doctrine of implied repeal applied?

b) Next, Lord Reed concluded that the claimants' arguments were misconceived (the putative conflict of domestic constitutional principle with EU law did not arise): see [80]-[116] in the course of which Lord Reed remarked *obiter* at [110] that the argument was problematic more generally since it conflicted with the separation of powers in many states; and at [111] that the approach of the BvfG in the Counter-Terrorism Database Act[18] was commended, if not applied. That approach suggested construing CJEU case-law in such a way that it did not call into question "*the identity of the national constitutional order*".

c) The joint judgment of Lords Neuberger PSC and Mance JSC also touched on this subject at [200]-[202] (presumption against a reading of CJEU case-law that would conflict with common separation of powers doctrines) before at [203]-[208] considering the position of conflict with "*other principles hitherto also regarded as fundamental and enshrined in the Bill of Rights*". Their conclusion was that "*the point is too important to pass without mention. We would wish to hear full argument upon it before expressing any concluded view.*"

61. The case of *Pham v Secretary of State for the Home Department* [2015] UKSC 19, [2015] 1 WLR 1591 ('***Pham***') was decided some 14 months later; in many ways it constituted a re-run of the issues also canvassed in the Court of Appeal in the case of *GI (Sudan) v Secretary of State for the Home Department* [2012] EWCA Civ 867. A variety of Treaty Declarations (summarised at [86]-[89] *per* Lord Mance JSC) from 1972 onwards had emphasised that EU law did not touch upon or shape domestic laws on British nationality/citizenship, such that the concept of EU citizenship (when introduced by the Treaty of Maastricht in 1992) in what is now Article 20 TFEU was entirely derivative. Early CJEU case-law (C-192/99 *Kaur*) accepted this without qualification; but a later case, C-135/08 *Rottmann* appeared to suggest that a withdrawal of nationality that led to a loss of EU citizenship would be subject to control by EU law, and specifically the

[18] BvfG (German Federal Constitutional Court) judgment of 24 April 2013 on the Counter-Terrorism, found in official English translation at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2013/04/rs20130424_1bvr121507en.html

proportionality principle. The key reasoning (that of Lord Mance JSC), as to the first premise of the Claimant's argument (i.e. that EU law applied) was as follows:

a) At [82] Lord Mance drew upon *HS2* and identified the separate tasks of interpretation and the conferral of jurisdiction (*kompetenz-kompetenz* by another name).

b) At [83] he set out the key provisions in the TEU relating to the principle of conferral of jurisdiction on the EU, namely Articles 4 and 5.

c) At [84] he identified that "*it is clearly very arguable that there are under the Treaties jurisdictional limits to European Union competence in relation to the grant or withdrawal by a member state of national citizenship*" before setting out at [85]-[89] the various Declarations and Decisions that had at each stage accompanied the conferral of new powers.

d) At [90] Lord Mance then noted:

> *A domestic court faces a particular dilemma if, in the face of the clear language of a treaty and of associated declarations and decisions, such as those mentioned in paras 86 – 89, the Court of Justice reaches a decision which oversteps jurisdictional limits which member states have clearly set at the European Treaty level and which are reflected domestically in their constitutional arrangements. But, unless the Court of Justice has had conferred on it under domestic law unlimited as well as unappealable power to determine and expand the scope of European law, irrespective of what the member states clearly agreed, a domestic court must ultimately decide for itself what is consistent with its own domestic constitutional arrangements, including in the case of the 1972 Act what jurisdictional limits exist under the European Treaties and on the competence conferred on European institutions including the Court of Justice.*

e) He then indicated (following the BvfG Counter-Terrorism Database approach again) that such problems would be avoided by careful co-operation and consideration (necessarily by the CJEU) of the Declarations which were precursors or qualifying conditions on conferral of additional powers, before concluding the problem did not require resolution since the Claimant's argument failed on its second premise (that EU law added materially to the legal protections in play), noting:

> *I am satisfied that this is not the occasion to attempt any such task, unless and until the second premise is established and involves a conclusion that Union law not only offers advantages over the relevant domestic law governing removal of the claimant's citizenship, but offers advantages which are or at least may be critical to the success of the claimants case.*

62. What links both such speculative and *obiter* passages in *HS2* and *Pham* is a clearly identifiable domestic constitutional tenet or axiom around which a principled argument can be made that the powers the CJEU claims were not conferred as a matter of domestic constitutional law:

    a) In *HS2*, it could be argued that Article 9 of the Bill of Rights embodies a fundamental UK constitutional principle which the Supreme Court has in effect ruled to be incapable of implied repeal (using the now strengthened common law principle of legality), even by another constitutional statute like the ECA 1972. This is either a check upon initial conferral of powers or, more plausibly, a qualification upon or limitation to the extent to which EU law is given effect by the ECA 1972.

    b) In *Pham*, the Declarations demanded by the UK and others as a price for the conferral of additional competences on the EU in relation to citizenship contained express *renvoi* to national law definitions of citizenship; and Article 20 TFEU was parasitic upon the concept of nationality so defined. Such construct of EU citizenship built only upon prior national citizenship (given the constitutional nature of citizenship identified by Laws LJ in *GI (Sudan)*) constitutes, it might be argued, implied limit on the jurisdiction of the CJEU, which was necessarily not competent to rule upon the requirements of national citizenship law.

    Barring such circumstances, it will require an express statement from Parliament (and thus an assertion of Parliamentary sovereignty) to deprive s.3(1) of the ECA 1972 of the effect identified in *Factortame No.2* which is to give effect to the supremacy of EU law, and CJEU rulings upon it in all circumstances.

63. In the present case there is no equivalent constitutional principle around which to build any a domestic constitutional *kompetenz-kompetenz* or conferral argument for the following simple reasons:

a) There is no domestic constitutional principle that says the Agencies or the Secretary of State when acting in the field of national security are amenable only to domestic control. Indeed, the EU has exercised such control for decades. Parliament has full power to decide what limits to set over national security powers (whether directly or through others) and to decide which courts can police those rules. This Tribunal's exclusive jurisdiction under s. 65(1) of RIPA to hear HRA 1998 cases involving the Agencies is proof positive of that proposition. As such there is no basis in domestic law to limit the wide language of the ECA 1972.

b) The only candidate provision for a *kompetenz-kompetenz* argument is thus Article 4(2) TEU, a provision of pure EU law which addresses in general terms the topic of conferral. It is a provision that the CJEU has repeatedly considered and addressed, both in *Watson* itself **[AS1/17]**, *ZZ* **[AS1/13]**, as well as in [80]-[84] of the Opinion of AG Sharpston in *IN* ECLI:EU:C:2016:85, and found not to rewrite the long-standing *acquis* on the controls that EU law applies when national security is invoked to derogate from or alter EU rights and obligations.

c) Article 4(2) TEU stipulates only two things that are material for present purposes: respect of the essential state functions of Member States, including safeguarding national security; and Member States have sole *responsibility* for national security. The identification of "sole responsibility" is not and cannot be a wholesale *renvoi* to national law. Nor is it the same as saying that the topic of national security as a whole remains entirely out of the scope of the Treaties. Either such reading of the provision would have been: (a) to reverse many years of consistent *acquis communitaire* and (b) to render nonsensical a number of Treaty provisions and of the large volume of EU delegated legislation that has made special provision for national security as a legitimate ground for exemption or derogation from EU rights and obligations.

d) Once it is appreciated that national security comes into the scope of EU law whenever deployed as a *derogation* from a private party's EU rights and obligations; and that such derogation must be consistent with EU requirements (Charter compliance, proportionality etc.), it is clear that there is a distinction

between: EU control or limits over national security powers, if and when asserted in a case falling in the scope of EU law and residual member state responsibility to protect the state and its citizens.

e) Beyond Article 4(2) TEU, the only argument open to the Respondents is to contend that in *all respects* the national courts determine all questions about the proper interpretation of powers conferred in the Treaties. But such a wide argument (which does not appear to have been advanced) is unsustainable in the light of the clear wording of ss.2 and 3 ECA 1972, which show that in principle Parliament has assigned this task (as a matter of domestic law and pursuant to Parliamentary sovereignty) to the CJEU. Moreover, such a wide argument is impossible to reconcile with either *HS2* or *Pham* where the Justices were careful merely, in inconclusive and/or *obiter* passages, to describe *potential arguments*; and to do so in conspicuously narrow terms grounded in well-established fundamental domestic constitutional principles or areas of reserved national competence clearly defined by express *renvoi* to national law in the Treaties themselves/their Declarations.

f) Indeed, here any doubt is resolved by Parliament's express step in subjecting s.94(1) and (2) general and particular Directions to justification by reference to the EU concept of proportionality; a change plainly made by the Communications Act 2003 to ensure compliance with the CRF. Such can only be taken as Parliamentary acceptance of the application of EU law to this form of Direction, just as EU law applies to a gamut of other Direction-making powers under the Communications Act 2003 and various Wireless Telegraphy Acts: see e.g. ss.1-5 Communications Act 2003.

(b) Remedies

64. The proper remedy for the IPT to adopt, if it considers *Watson* to be wrongly decided (whether on Article 4(2) TEU jurisdictional grounds, or by dint of the safeguards required by the CJEU to comply with Articles 7 and 8 of the EU Charter) is to declare itself bound by the principles clearly expressed therein, by dint of s.3 ECA 1972 and

Factortame No.2 whilst expressing the view that the CJEU decision is wrong. It will then be for Parliament (which can make express exemption or provision should it so choose).

65. The Respondent proposes two means by which this Tribunal can, if applicable, express its view that the decision in *Watson* exceeds jurisdictional bounds:

a) It can in engage in a form of purposive construction of the CJEU judgment – a reading down akin to that performed under s.3(1) HRA, the common law presumption of legality or under the EU *Marleasing* doctrine. This is in truth "reverse Marleasing", the very antithesis of the approach to EU law that the CJEU case-law (binding by dint of s.3(1) ECA) requires.

b) Or there can be some form of decision that the judgment in *Watson* is *ultra vires*, and so simply does not bind the IPT at all.

66. These are both remedies predicated upon a prior assessment that the CJEU has exceeded its jurisdiction/erred in its identification of conferred powers. Neither remedy has any domestic precedent; both are on their face inconsistent with the express demands of ss.2 and 3 ECA, as interpreted by the House of Lords in *Factortame No.*2, a decision that binds this Tribunal.

67. Quite apart from the binding precedent supplied by *Factortame No. 2*, the Claimant suggests that it would be constitutionally inappropriate for this Tribunal – one of limited jurisdiction from which no appeal lies[19] – to engage upon either step which would be of extreme constitutional moment. The Supreme Court has clearly flagged in *Pham* and *HS2* its willingness to engage with such issues in what it considers to be an appropriate case; and it is that Court that should have the ultimate say over such arguments, not least for their likely critical bearing in any Brexit negotiations. Indeed, only that Court,

[19] And see *R (Privacy International) v Investigatory Powers Tribunal* [2017] EWHC 114 (Admin), which is on appeal to the Court of Appeal, deciding that decisions of the Investigatory Powers Tribunal were not amenable to judicial review.

pursuant to the 1966 Practice Direction[20], can qualify the binding effect of *Factortame No.2*.

68. Moreover, the interpretative remedy is unworkable on the facts. The UK addressed the CJEU on Article 4(2) TEU, and the CJEU plainly had Article 4(2) TEU in mind. It structured (and then corrected) the *Watson* judgment to address use both to combat serious crime and for national security purposes. Given the common thread of terrorism in both topics, and given that the use of BCD upon which the Respondents' pin their case (identifying persons of interest for terrorist investigations), it is impossible in any event to draw a sensible distinction between the two topics. Further, the content of s.94(2A) TA 1984, and the plain acceptance that such section 94 Directions were within the scope of EU law works fatally against any contention that such approach is consonant with Parliament's supposed true intention.

69. Even were the IPT inclined to follow one of these courses (which it should not, as the *kompetenz-kompetenz* argument is misconceived) it would be unlawful and wrong in principle for it do so without first having referred further questions to the CJEU pursuant to Article 267(3) TFEU (the IPT being a final court for these purposes):

a) First, the only hook for the Respondents' argument is Article 4(2) TEU, a provision of pure EU law, inserted for the benefit of all 28 Member States. The interpretation of this provision – and the extent to which it excludes the operations of national security agencies from the scope and application of EU law – is a question of pure EU law. There is, as already explained, no special domestic constitutional principle in issue.

b) Second, if the IPT considers the answer given in *Watson* is wrong in law, and leads to an excess of jurisdiction from the perspective of Article 4(2), it should explain its reasons in a judgment and give the CJEU the opportunity to engage with such reasoning, answering or accepting it. This is the course that the BvfG

[20] The Practice Statement (Judicial Precedent) [1966] 1 WLR 1234 "*has as much effect in [the Supreme] Court as it did before the Appellate Committee in the House of Lords*": *Austin v Mayor and Burgesses of the London Borough of Southwark* [2010] UKSC 28 at [24]-[25].

recently followed in the reference it made in Case C-62/14 *Gauweiler* ECLI:EU:C:2015:400.[21] It is, on any view, the very least the duty of loyal co-operation in Article 4(3) TEU (replacing the old Article 10 EC) requires; and, if one is to take a step as radical as declaring a recent decision of the Grand Chamber of the CJEU *ultra vires* based on a novel re-interpretation of Article 4(2) TEU, it should be reached only after the mechanism allowing all 28 signatories to the Treaty, who benefit equally from this provision, to be heard.

c) Third, *da Costa* establishes that a national court otherwise bound by an 'on point' ruling of the CJEU retains the power and discretion to refer what are in essence the same or very similar questions to those previously answered, for instance if it thinks the earlier ruling to be wrong.

d) Fourth, the effect of accepting a *kompetenz-kompetenz* argument would be in effect to declare that Article 15(1) of the e-Privacy Directive insofar as it deals with national security is *ultra vires* Article 4(2) TEU. This is a matter within the exclusive competence of the CJEU, which must be given the opportunity to consider the issue. See *FotoFrost* [1987] ECR 4199.

e) Finally, such course is obviously preferable when the chronology (and past jurisprudence touching on national security, notably *Floe Telecom*) suggest the Respondents' real complaint is not of an excess of *jurisdiction* but rather that the CJEU overextended the *substantive content* of Articles 7 and 8 of the EU Charter in *Watson*. If the IPT considers that contention has any substance it can and should be put to the CJEU, not least because the alternative (i.e. refusal to recognise *Watson*) terminates judicial dialogue, and will present huge complexities (and risk grave damage to UK commercial interests) during and after Brexit not least because of what David Anderson QC has aptly called the 'Hotel California'[22]

---

[21] See also the questions referred at http://curia.europa.eu/juris/document/document.jsf?text=&docid=150354&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1008256; the Respondents could no doubt supply the full Order for Reference as translated, which make it plain that the BvfG raised the *kompetenz kompetenz* point squarely: see Tridimas, *loc cit*, pp.420-424.

[22] D Anderson QC, '*Terrorism: the EU picture*', Counsel Magazine (May 2017) 25-26. For any reader not as familiar with 70s Californian rock as Mr Anderson QC: "*Last thing I remember, I was running for*

created by the *Schrems* ruling, which will preclude data sharing with the UK once it becomes a third country for so long as it fails to comply with EU data protection standards. As Mr Anderson QC puts it:[23]

> *Put bluntly, the UK will not be trusted with the personal data of EU citizens unless it can demonstrate that it will afford those data equivalent protection to that which is available in the EU. Recent EU case law in this field, which prioritises data privacy over operational efficacy, will thus remain problematic even after Brexit. In this, as in some other respects, the EU looks set to prove a 'Hotel California', from which we will check out but which we will never entirely leave.*

(iii) The Respondents' argument that *Watson* can be distinguished

70. The Respondents submit that, even if the DPD and/or EPD were engaged by section 94 Directions, *Watson* should be distinguished on the basis that a different proportionality balance may be struck in respect of such processing in the interests of national security.

71. This argument is untenable. DRIPA *was* national security legislation. The suggestion that DRIPA and *Watson* were about criminal investigation alone is wrong. DRIPA expressly permits a retention order to be made for the purposes of national security.[24] It is to be assumed that DRIPA retention orders have been made for national security purposes. The CJEU was well aware of the use of DRIPA for national security purposes.[25]

72. The suggestion that the power under s.94 TA 1984 is materially different to the power to issue a DRIPA retention notice is equally hopeless. Both national provisions are used to impose a requirement on a CSP to retain and process data. Both therefore fall within the scope of EU law, for the reasons given in *Watson* at §78. A direction under s.94 is an obligation on a CSP to process data in a manner that breaches (at least) Article 5 and 6(4) of the e-Privacy Directive.

---

the door, I had to find the passage back to the place I was before, 'Relax' said the night man, 'We are programmed to receive'. 'You can check out any time you like, but you can never leave.'"

[23] D Anderson QC, '*Terrorism: the EU picture*', Counsel Magazine (May 2017) at 26.

[24] See fn 10 above.

[25] The above domestic statutory regime was set out by the CJEU in *Watson* at §§29 and 33.

73. Further, it is a key part of the Respondents' case on sharing that they are entitled to take BCD obtained for national security purposes and share it for other purposes, such as the detection of serious crime. Indeed, they have admitted that they do so. As such, the argument that BCD obtained under s.94 TA 1984 is somehow 'set apart' because of the national security basis of the direction is not open to the Respondents; BCD is used for purposes other than protecting national security.

74. The Respondents have also put in evidence suggesting that it would be impractical to comply with the *Watson* safeguards in the context of national security: see the third witness statement of the GCHQ Witness dated 2 March 2017 **[Supp2/11]**. Such evidence obviously has no bearing on the legal question of whether *Watson* applies to section 94 Directions. But in any event, the evidence is incorrect for the reasons explained in the second witness statement of Camilla Graham Wood at §§29-49 **[Supp 2/10/8-12]**. There is no reason to think that practicable implementation of the requisite safeguards could not be achieved by the Respondents.

(iv) Conclusion

75. The Respondents' various alternative submissions on *Watson* fail at each hurdle. It is not enough, as the Respondents seem to think, merely to assert that national security falls outside the scope of EU law. Where a PCN/PECS is required to carry out processing (as defined under the DPD), such request must comply with EU law – there is no basis to distinguish such a request being made under s.94 TA 1984 from a request being made under DRIPA. Nor is there scope for distinguishing such a request for BPDs from commercial actors. Nevertheless, if the Tribunal is considering deciding that the CJEU has acted outside its jurisdiction in so finding, or has simply got the law wrong in *Watson*, it must first refer this matter to the CJEU under Article 267(3) TFEU.

III. SHARING BPD AND BCD WITH THIRD PARTIES

76. This Tribunal held in its October 2016 Judgment at §95, underlining added **[AS1/24]**:

> *The only area in which we need to give further consideration relates 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. There are detailed provisions*

in the Handling Arrangements which would appear to allow for the placing of restrictions in relation to such transfer upon the subsequent use and retention of the data by those parties. It is unclear to us whether such restrictions are in fact placed, and in paragraph 48.2 of their Note of 29 July 2016 the Respondents submit that the Tribunal is not in a position to decide this issue. We would like to do so and invite further submissions.

77. The issue in *Liberty/Privacy (No. 1)* [2015] 1 Cr App R 24 **[A2/38]** was the legality of the regime for *receipt* of intercept material collected by foreign partners. This case concerns the reverse situation: what standards and safeguards apply to bulk data which is given to third parties? Indeed, BPDs may well contain intercept material; it has been avowed that some BPDs are obtained by interception (see paragraph 28(a) above).

A. Facts

78. There are two different ways in which BCD and BPD may be shared with third parties:

a) Transfer. The third party receives a copy of the data which has been selected for sharing: a legal analogy might be giving someone a copy of the entire set of the Law Reports.

b) Remote access. The third party is given the ability to access remotely the Agencies' own databases, allowing for querying and search of SIA databases: a legal analogy would be giving someone a username and password for Westlaw or LexisNexis, allowing for searches of a database held elsewhere.

79. Each method may be used by the Agencies. This is avowed. See GCHQ Exhibit 3 ("*the Agencies may share applications…*" **[Supp1/7/1]**) and MI5 Exhibit 2 ("*Sharing data and applications in situ* [REDACTION] *Sharing data in this way requires both the requesting and disclosing agencies to assess the necessity and proportionality of the access and use being sought* [REDACTION] *The senior MI5 official should be consulted in relation to any proposals to… allow SIA access into MI5 systems…*" **[Supp1/8/3]**).

80. It is common ground that GCHQ discloses entire databases of "*raw sigint data*" to "*industry partners*" who have been "*contracted to develop new systems and capabilities for GCHQ*" **[3/476]**. It is avowed that there are "*frequent releases of routine sets of raw Sigint*

data to industry partners" **[3/476]**. When this occurs, there appear to be few safeguards. For example, there appears to be no requirement for each search to be explained and justified in writing. Security clearance is required only "*wherever possible*" **[3/476]**.

81. It is clear that at least one CSP has been sufficiently concerned to demand that foreign sharing of its customers' BCD did not occur:

> "*In one case a PECN had asked the agency to ensure that that* [sharing with other jurisdictions] *did not happen and we were able to confirm that their data had not been shared with another jurisdiction. In other cases PECNs stated they would be very concerned if their data was shared with other jurisdictions without their knowledge*" (Burnton Report, §6.7 **[A4/82]**)

82. Further, the Agencies share bulk data with foreign partners, in particular the Five Eyes countries. The pretence of "neither confirm nor deny" is maintained as to the fact of outward (but not inward) sharing. But this NCND plea is unreal in light of materials now in the public domain. GCHQ disclosed a revised "*GCHQ Policy for Staff from OGDs and SIA partners with access to GCHQ systems and data*" on 11 May 2017. Paragraph 9 avows receipt of "*Sigint and non-Sigint data*" from "*the 5 Eyes partners*" to GCHQ.

83. The Five Eyes relationship is governed by the UKUSA agreement. The UKUSA agreement is in the public domain. It explains that Five Eyes is a reciprocal sharing partnership. See Article 4 and Appendix C, para. 3 ("*each party will continue to make available to the other continuously, currently, and without request, all raw traffic*…"). It is also avowed that BPD may be obtained by interception (David Anderson QC, *Bulk Powers Review*, footnote 119 **[AS1/27/48]**). Accordingly, it has now been confirmed by official sources that there is sharing of data held in BPDs with the Five Eyes foreign partners.

84. The Snowden documents[26] contain more detail of the types and extent of information sharing that take place, and the risks involved. For example:

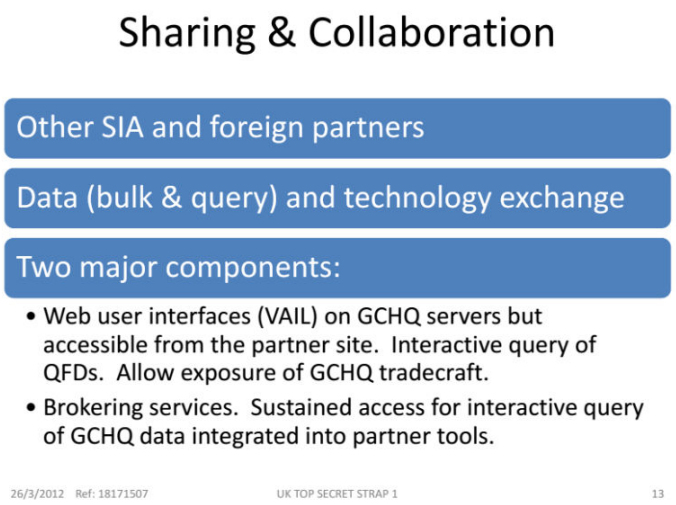
---

[26] These documents are in the public domain and accordingly can be used in these proceedings: *R (Bancoult) v Secretary of State for Foreign and Commonwealth Affairs* [2013] EWHC 1502 (Admin) at [35]. Where the Claimant refers to a redacted version of such a document, the Tribunal is asked to look in CLOSED at the original and unredacted version of that document.

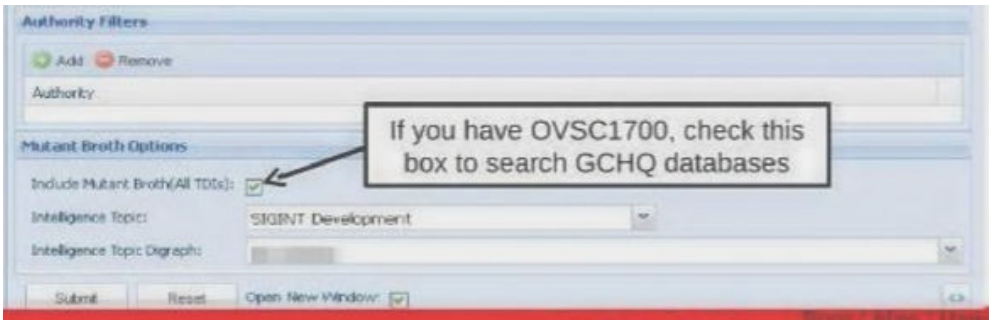
a) The Director of the NSA was briefed that Sir Iain Lobban (former Director of GCHQ) was likely to ask about whether UK-sourced data might be given by the NSA to, for example, the Israeli government, to conduct "*lethal operations*". The fact that GCHQ needed to ask such questions indicated that appropriate safeguards were not in place at the time of transfer:

- (TS//SI//NF) **UK Intelligence Community Oversight**: GCHQ and its sister intelligence agencies are challenged with their activities and operations being subject to increased scrutiny and oversight from their government (and public). As a result, closer attention is being paid to how UK-produced intelligence data is being used by NSA, and other partners. It is possible that Sir Iain may ask about what safeguards NSA may be putting in place to prevent UK data from being provided to others, the Israelis for instance, who might use that intelligence to conduct lethal operations. *For additional information about this subject, and other UK Intelligence Community legal issues and legislation, see the attached paper prepared by Mr.* [redacted]*, Office of the General Council, London.*

b) GCHQ documents confirm that sharing takes place with other Agencies and foreign partners, including data transfers in bulk and remote access. GCHQ provide "*web user interfaces*" that are "*accessible from the partner site*" and offer "*sustained access for interactive query… integrated into partner tools*":



c) For foreign partner agencies in the Five Eyes, access to GCHQ's databases is as simple as ticking a box on a computer form. The only requirement at the NSA is to have completed a training exercise, known as OVSC1700:



d) One particularly important industry partner is the University of Bristol. Snowden documents indicate that researchers are given access to GCHQ's entire raw unselected datasets, including internet usage, telephone calls data, websites visited, file transfers made on the internet and others. Researchers are also given access to GCHQ's entire targeting database ("*delivered… at least once a day…*"), an exceptionally sensitive dataset:[27]

F.1.1 SALAMANCA

The contents of this dataset are classified TOP SECRET STRAP2 CHORDAL.

GCHQ collects telephone call record events from a wide variety of sources, and these are stored in a database called SALAMANCA [W36]. This data is also fed to the SUN STORM cloud and the BHDIST DISTILLERY cluster (and other DISTILLERY clusters). This data is a relatively low rate feed of user events, around 5000 events per second, and can be viewed as

F.1.2 FIVE ALIVE

FIVE ALIVE is an ICTR prototype Query Focused Dataset (QFD) providing access to bulk IP-IP connection events, giving a unique unselected view of all activity on SIGINT bearers. Each record in FIVE ALIVE summarises a *flow* between two IP addresses. This summary

F.1.3 HRMap

The contents of this dataset are classified TOP SECRET STRAP2 CHORDAL.

When a user requests a webpage from the internet, this is observed in SIGINT as an HTTP GET request. As well as the page requested it often contains the URL of the previously viewed page. The hostname of the requested page is the "HOST" and the hostname of the previous page is the "REFERRER". When we consider just the hostnames rather than the full URI then this is considered events data. This can be viewed as a directed graph of hostnames, and is given the name HRMap at GCHQ. It is a moderately high rate stream (around 20000 events per second) which should be suitable for the streaming EDA and streaming expiring graphs topics.

27 The extracts below are curtailed at F.1.1, F.1.2 and F.1.4.

> **F.1.4 SKB**
>
> *The contents of this dataset are classified* TOP SECRET STRAP2 CHORDAL UKEO.
>
> The Signature Knowledge Base is a system for tracking file transfers made on the internet. A record is made each time we see certain file types being transferred. Each file is identified by its format and a hash of some of its content. Whilst this does mean we can store the data,
>
> **F.3.2 Target selectors**
>
> *The contents of this dataset are classified* TOP SECRET STRAP2 UKEO.
>
> Our target knowledge database is BROAD OAK which includes the ability to task various selector types including phone numbers and email addresses. The resulting list of selectors is sometimes called the target dictionary and is delivered to our DISTILLERY clusters at least once a day, and is also available on our Hadoop clusters. This data could be used to see if some result set contains an increased density of targets.

e) Other UK agencies, such as HMRC, are given access to GCHQ data via the 'MILKWHITE Enrichment Service'.[28]

85. These methods of sharing each carry distinct but overlapping risks:

a) Transfer results in the Agencies losing control of how the data is used, stored, retained, disclosed or destroyed. As the Intelligence and Security Committee accurately put it, "… *while these controls apply within the Agencies, they do not apply to overseas partners with whom the Agencies may share the datasets*") (§163 **[A4/79]**). Once the data has been handed over to the third party, it could be deployed in support of an unlawful detention or torture programme, in the violent interrogation of a suspect, or used to identify a target for a lethal operation. It may be (overtly or covertly) passed onto another country, even though the UK would be unwilling to share directly with that state. There is no evidence that the control principle is operated or respected by the partners with whom data is shared.

b) Permitting remote access allows the third party to quickly search vast quantities of data which remains on the Respondents' systems. The third party gets all the benefits of access to the Agencies' systems and the power and intrusiveness of

[28] See the witness statement of Caroline Wilson Palow, §§7-11 at **[5/2/25-26]**. See also: https://edwardsnowden.com/2016/10/28/milkwhite-enrichment-services-mes-programme/.

access to indexed and searchable material, without having to process the data itself.

86. It appears that there is little, if any, oversight by the Commissioners in respect of either transfer of BCD or BPD to other agencies or remote access to it. In particular, it is unclear whether the use of shared data is even auditable, or audited in fact. The Interception of Communications Commissioner has started an investigation into sharing of intercept material, but not yet reported (*Annual Report for 2015* (July 2016), §6.83 **[AS1/28/36]**). It is unclear if the investigation has been progressed or completed. There is nothing in the Intelligence Services Commissioner's reports that indicates that any audit or analysis of what data has been shared has taken place. Disclosure has been requested in correspondence with the Tribunal.

B. Article 8 ECHR

87. Any sharing prior to avowal was unlawful, for the reasons given in the October 2016 Judgment.

88. The arrangements after avowal still do not comply with the *Weber* criteria. Any interference with Article 8 must be "*in accordance with the law*" (see Article 8(2)). This requires more than merely that the interference be lawful as a matter of English law: it must also be "*compatible with the rule of law*": *Gillan v United Kingdom* (2010) 50 EHRR 45 **[A3/58]** at §76. There must be "*a measure of legal protection against arbitrary interferences by public authorities*", and public rules must indicate "*with sufficient clarity*" the scope of any discretion conferred and the manner of its exercise: *Gillan* at §77.

89. In *Weber & Saravia v Germany* (2008) 46 EHRR SE5 **[A3/53]**, the ECtHR held at §§93-94:

> *The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures … Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its*

exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

90. In *Weber*, the Court at §95 referred to the minimum safeguards in order to avoid abuses of power, including the need for safeguards on sharing:

> *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: … the precautions to be taken when communicating the data to other parties.*

91. There are no restraints in primary legislation on the sharing of bulk data:

a) Section 19 of the Counter Terrorism Act 2008 (the '**2008 Act**') **[A1/9]** permits sharing and onward disclosure and the use of material obtained for one purpose for another. Sharing of information pursuant to section 19 of the 2008 Act does not require any warrant or other external authorisation, regardless of the private or sensitive nature of the information. There is no requirement for oversight of a decision to share information under section 19.

b) If a BPD contains intercept material, the basic safeguards in section 15(2) and (3) of RIPA limiting the number of persons to whom the material is disclosed, the extent of copying and arrangements for destruction may be disapplied by the Secretary of State. The Secretary of State may decide to retain such requirements "*to such extent (if any) as the Secretary of State thinks fit*" (section 15(7)(a) of RIPA **[A1/7]**).

c) Nothing in s.94 TA 1984 imposes any restriction on sharing.

d) The Data Protection Act 1998 ('**DPA**') has been abrogated by ministerial certificate. The eighth data protection principle provides "*Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data*". That principle is disapplied by each of the Agencies' certificates made under section 28 of the DPA. For example, GCHQ's certificate **[3/17-20]** provides for the following exemption:

PART A			
Column 1		Column 2	
1.	Personal data processed in the performance of the functions described in section 3 of the Intelligence Services Act 1994 ("ISA") or personal data processed in accordance with section 4(2)(a) ISA.	i) ii) iii) iv) v)	Sections 7(1),10 and 12 of Part II; Sections 16(c), 16(e), 16(f),17,21,22 and 24 of Part III; Part V; the first data protection principle; the second data protection principle;
2.	Personal data relating to the vetting of candidates, staff, contractors, agents and other contacts of GCHQ in accordance with the Government's security and vetting guidelines and policy including but not limited to:	vi) vii)	the sixth data protection principle to the extent necessary to be consistent with the exemptions contained in this certificate; and the eighth data protection principle.

92. Nor is there any secondary legislation or Code of Practice providing safeguards over the sharing of BPD or BCD.

93. There are three reasons why this situation is in breach of Article 8 ECHR:

a) it constitutes a circumvention of the limited safeguards in the TA 1984, RIPA and DRIPA;

b) the absence of foreseeable rules and safeguards; and

c) the inadequacy of those safeguards.

94. A section 94 Direction may be made only if '*necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom*'; on the face of the statute, the BCD direction may be made only for national security/international relations purposes. However, the ability to share data so acquired for other purposes circumvents this restriction:

a) As explained above, neither a body such as HMRC nor the agencies could obtain a section 94 authorisation for a non-national security purpose, such as the detection of tax evasion. Other powers exist to obtain communications data for that purpose, in Part I, Chapter II of RIPA.

b) If GCHQ and/or MI5 give access to their section 94 data to HMRC, for the purposes of detecting tax evasion, HMRC is circumventing the RIPA safeguards. HMRC and the NCA could have requested and obtained communications data

themselves under RIPA. The effect of getting access to the same data under section 94 is to circumvent the protection of the Designated Person, the SPoC, the Interception of Communications Commissioner and the other safeguards in the Codes of Practice.

c) Such circumvention is not compatible with Article 8 ECHR. In *Liberty/Privacy (No. 1)* **[A2/38]** the Tribunal held that Agencies must apply the RIPA safeguards by analogy when obtaining information from a foreign partner. This was common ground: see [30] and [53]. Where there was no procedure to ensure that RIPA safeguards were always implemented, such a procedure had to be introduced.

95. Moreover, such use also circumvents the safeguards provided by DRIPA and the Regulations made under it, which built upon the basic architecture of RIPA. For instance, such 'recycling' of BCD would enable the Security Services to share data retained by it beyond the 12-month limit applicable to bodies bound by section 1(5) of DRIPA. Such a use, of an obscure and very generally worded power, to circumvent an express statutory safeguard in a regime designed for and addressing the very topic in hand (data retention for access for subsequent authorised official access to investigate crime) is obviously unlawful.

96. Second, the arrangements are not sufficiently foreseeable. 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. It was only in March 2017 (in response to RFIs) and in April 2017 (in evidence) that limited disclosure was given in the most general terms about the approach of each of the Agencies to sharing, and even then on a hypothetical basis. Until the present hearing, such materials have not been in the public domain. Even now, it is unclear what the policy of MI5 and MI6 in fact is. It appears that GCHQ operates a policy requiring that sharing partners adopt a level of protection "*equivalent*" to GCHQ's own safeguards. No clear answer has been given to the RFI asking whether MI5 and MI6 operate the same requirements. It appears that they only do so "*insofar as considered appropriate*" (Response to RFI 10 May 2017, paras. 7, 10), which is unilluminating.

97. The Claimant has made further efforts to attempt to discover the outline of the applicable policy. In the Claimant's skeleton for the directions hearing on 5 May 2017 it said:

> *As to sharing, the Claimant's understanding is that GCHQ has an internal policy requiring the recipients of such bulk datasets to have equal safeguards to GCHQ's own safeguards; however, neither MI5 nor MI6 have such a policy, instead operating an entirely discretionary internal process. It is also understood that, unlike the provision under s. 12 of RIPA 2000 or (the broader provision) under s. 171(9) of the Investigatory Powers Act 2016, there is no requirement for the Secretary of State personally to authorise transfer to a body which derogates from the safeguards specified in domestic law. If the Respondents confirm that the Claimant's understanding is correct, the Claimant will not need to request further information on these topics at this stage; and can make substantive submissions accordingly.*

98. The Respondents were ordered to provide a response to this paragraph.[29] The GLD replied on 10 May 2017 indicating that "*the Respondents to do not give the confirmation requested*". The arrangements are therefore still not foreseeable because the actual policy of MI5 and MI6 remains opaque. It is not clear whether:

a) Secretary of State approval is required as indicated above; or

b) MI5 and MI6 in fact require equivalent standards when sharing datasets.

99. Finally, the safeguards are inadequate.

100. Two issues arise. First, the Claimant assumes in the absence of a clear response that the policy of MI5 and MI6 does not in fact require equivalence, in contrast to that operated by GCHQ; nor is the approval of the Secretary of State required for any deviation from equivalence. If so, such standards are plainly inadequate to protect against arbitrary conduct. When an entire dataset (mostly consisting of information about people about whom there is no legitimate intelligence interest) is handed over to a commercial, foreign or UK partner (notwithstanding the question of proportionality of such action), it is essential that high standards are applied. If the standards applied are worse than

[29] Paragraph 1(c) of the Tribunal's Order dated 5 May 2017.

those operated by the agencies (perhaps in terms of oversight, security or the protection of privacy) it is impossible to see how the sharing is lawful.

101. Second, a crucial factor is likely to be the presence or absence of oversight and control:

a) Has the Commissioner reviewed and audited the sharing of data? There is no evidence of any such review or audit in any of the published reports.

b) Is the use made of the shared data auditable and audited?

c) Has any misuse been discovered?

d) Would a claim to the Tribunal identify such misuse, or would the Tribunal's standard searches fail to detect misuse?

e) If and where controls are applied, how do the Agencies prevent information being used improperly, such as in support of an unlawful rendition operation, mistreatment or torture?

f) How do the Agencies and the Commissioner check whether or not a researcher at a commercial partner or HMRC has (like a number of intelligence officers) carried out an unlawful search of bulk data to find out about the movements and internet use of a friend, partner or family member? Have they ever done so?

102. On Friday 12 May 2017, the Tribunal wrote to the Commissioners asking them to give an OPEN response on the extent of the audit they have carried out. Further submissions will be made once a response is received.

C. EU law

103. The position under EU law is *a fortiori*. First, to the extent BCD is transferred out of the EU, this is unlawful following *Watson*: see §§114, 122 and 124 **[AS1/17]**.

104. Secondly, it is admitted that s.94 TA 1984 BCD (which can be obtained only for national security purposes) is repurposed for serious crime investigations that do not raise any national security issue. For example, HMRC may be given access to BCD or BPD under

the 'MILKWHITE' programme. In these circumstances, BCD is being collected and used for ordinary criminal investigations and the safeguards and standards in *Watson* must apply, even on the Respondents' own case.

105. Finally, where the information contained in a BPD is of a broadly equivalent level of intrusiveness to communications data, the principles of necessity and proportionality will require an equivalent level of safeguards governing access to data as those identified in *Watson*. See paragraph 27 above, and the opinion of Advocate General Mengozzi in *Opinion 1/15* **[AS1/18]**.

IV. PROPORTIONALITY

A. Bulk Powers Review

106. A useful starting point is David Anderson QC's *Bulk Powers Review* (August 2016), which examined the "*operational case*" for such powers **[AS1/27]**. Crucially, Mr Anderson QC was not permitted to opine on safeguards, nor make any assessment of proportionality (§9.8 **[AS1/27/121]**):

> *"It is not the function of this Report to pronounce on the overall case for bulk powers. The Government has been clear that "consideration of the safeguards that apply to [the bulk] powers, and associated questions of proportionality" should not form part of this Review…"*

107. Mr Anderson QC concluded that there was a good "*operational case*" for BPD and BCD generally, but noted that better oversight was required **[AS1/27/126]**:

> **Reducing the privacy footprint**
> *9.23 Also in need of technological expertise are the IPC inspectors whose task it will be to audit the disclosure, retention and use of material acquired pursuant to the new law (clause 205). Are the SIAs' systems equipped with "privacy by design" and if not what can be done about it? Could procedures be amended in such a way as to reduce privacy intrusion (for example by greater use of anonymised search results), without jeopardising operational efficiency? Such issues need a practical understanding of how systems are engineered, how powers are operated, and what could be done to minimise the privacy footprint of the SIAs' activities. The Bill already confers duties to audit, inspect and investigate. What is needed in addition is the expertise to enable those duties to be carried out in the most effective possible way.*

108. The absence of properly resourced technical audit of BCD and BPD demonstrates that there are not sufficient safeguards over the use of such powers, which are therefore both not in accordance with the law, and disproportionate. The following basic questions do not appear to have been considered:

a) How many 'failed searches' take place, where data is accessed but no useful intelligence purpose is served? Have the Commissioners examined the failure rate?

b) Have the Commissioners considered how the 'privacy footprint' of the use of BPD and BCD could be improved, and less data accessed?

c) What technical understanding do the Commissioners and the Tribunal have of the search techniques used by sharing partners? Are the searches and algorithms audited?

d) How are artificial intelligence techniques audited, if at all?

e) What examination have the Commissioners made of profiling, where information from multiple datasets is aggregated, in order to build a comprehensive profile about individuals and their activities?

109. These questions are all suitable for being dealt with in OPEN hearings, but, if necessary, the Tribunal should hear evidence and find facts on them in CLOSED. It is striking that, in their evidence, none of the witnesses called by the Agencies has made any attempt to address the proportionality of the use of BPD and BCD or how the privacy consequences of the collection and use of such datasets can be minimised.

B. Article 8 proportionality

110. Of course, an "*operational case*" does not equal proportionality. An excellent "*operational case*" can be made for a mandatory national DNA database, with a sample forcibly taken from every child at birth, or bulk retention of domestic communications content. Such schemes would nevertheless be unlawful:

a) In S & Marper v UK (2008) **[A3/54]** the UK noted that DNA data, which had proven to be of great value, would be deleted if the applicants were successful. Figures were provided (§92). The Court accepted that evidence (§§115-117) but nevertheless held that the retention of data was disproportionate (§§121-122). An "*operational case*" marks the start of an analysis of proportionality, not the end. A DNA fingerprint (which contains no personal information) is simply a unique identifier. It contains less intrusive personal information than a detailed record of a person's location and personal associations collected over several months, contained in BCD or BPD. Even though a sound 'operational case' may have existed, the retention was unlawful.

b) In MK v France (Application 19522/09) **[A3/56]** the Strasbourg Court at §40 again rejected the idea that blanket and indiscriminate retention of data was lawful "*accepting the argument based on an alleged guarantee of protection against potential identity theft would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant*".

The collection of BCD and BPD involves a more comprehensive and intrusive database than any previously considered by the Strasbourg court. A profile is built or capable of being built about any identifiable individual. The profile will reveal an individual's network of family, friends, business acquaintances, meetings and contacts and leisure and private activities. Accordingly, a scheme involving blanket retention of BCD or entire datasets of BPD, without independent authorisation, notification of usage or appropriate restrictions on scope is unlawful.

C. EU law

111. *Watson* is binding authority that the safeguards presently in place are inadequate. In particular, there is general and indiscriminate retention, no prior independent authorisation for access, no requirement for data to be retained in the EU and no notification provision.

THOMAS DE LA MARE QC

BEN JAFFEY QC

DANIEL CASHMAN

Blackstone Chambers

BHATT MURPHY

15 May 2017

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

B E T W E E N:

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

CLAIMANT'S SKELETON ARGUMENT
for hearing commencing 5 June 2017

Privacy International
62 Britton Street
London
EC1M 5UY

Bhatt Murphy
27 Hoxton Square, London N1 6NN
DX: 36626 Finsbury