Neutral Citation Number: UKIPTrib IPT_15_110_CH

No: IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

P.O. Box 33220
London
SW1H 9ZQ

Date: 8 September 2017

Before :

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

- -

Between :

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

- -

Hearing dates : 5, 6, 8 and 9 June 2017

- -

APPEARANCES

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

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

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

- - - - - - - - - - - - - - - - - - - -

APPROVED JUDGMENT

Sir Michael Burton (President) :

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

2. We gave a judgment, now reported at 2017 3 AER 647, on 17 October 2016 (the "October Judgment"), relating to the acquisition and use by the Security & Intelligence Agencies ("SIAs") of Bulk Communications Data ("BCD"), pursuant to s.94 of the Telecommunications Act 1984 ("S.94"), and of Bulk Personal Data ("BPD"). The issue before us was as to the lawfulness of the BCD and BPD regimes at domestic law, and by reference to the ECHR. The existence of BPD was first publicly avowed in March 2015 and of the BCD regime in November 2015. We concluded in the October Judgment that those regimes were lawful at domestic law, but that, by reference to Article 8 of the ECHR, they had not been lawful prior to their avowal. We concluded, subject to reservation of two issues by reference to the ECHR (proportionality and the arrangements as to transfer of data to third parties) to a further hearing, that since such avowal the regimes had been compliant with Article 8. We set out our consideration of the safeguards, which we found as facts and caused us to reach that conclusion, in paragraphs 85 to 101 of the October Judgment, with reference to the exercise of satisfactory supervision by the Interception of Communications Commissioner and Intelligence Services Commissioner since avowal and to the detailed arrangements for both regimes governing the SIAs, which we set out in an Appendix to the Judgment.

3. The parties were then, and are now, Privacy International, described, and represented, as set out in paragraph 2 of the October Judgment, and the

Respondents, the Foreign Secretary and the Home Secretary and the three SIAs (colloquially MI5, MI6 and GCHQ), as also there described and represented. We shall use the same abbreviations as were adopted in the October Judgment.

4. Apart from the two reserved issues as to the ECHR, the other issue, which was also then adjourned, has been addressed in detail at this hearing over the entire four days available for it, with the effect that the two ECHR issues have been further adjourned. It relates to whether the BCD and BPD regimes are within the scope of European Union Law ("EU Law"), and, if so, whether they comply with such law. At the time of the first hearing in July which led to the October Judgment, the decision of the Grand Chamber of the Court of Justice of the European Union (the "Grand Chamber") had not yet been given, but was subsequently given on 21 December 2016, in the case of **Watson** (joined cases C-203/15 and C-698/15 **Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson and Others**). As will be seen, we have concluded, for the reasons we give later in this judgment, that we should refer questions to the Grand Chamber pursuant to Article 267 of the Treaty on the Functioning of the European Union ("TFEU"). However, in the light of the submissions by the parties during the hearing, and the confirmation of the Respondents, it has not been necessary to refer any questions to the Grand Chamber in respect of BPD ("the BPD Position"), and the relevant considerations and conclusions which we set out below are concentrated upon BCD.

5. The BPD Position is as follows. The issue to which reference is to be made to the Grand Chamber relating to BCD concerns data in respect of which a commercial operator, engaged in an activity within the scope of EU law is compelled, by a direction enforceable by law, to provide to the SIAs data obtained in the course of ordinary business purposes in pursuing that business. This does not apply to BPD. The Respondents have confirmed that the SIAs do not use compulsory powers by reference to s.94 or any other similar power (e.g. the Airports Act 1986, the Transport Act 2000, the Civil Aviation Act 1982 or the Postal Services Act 2000) to obtain BPDs. With the exception of one historic occasion when BPD was obtained under s.94, which has been the subject of evidence, and which under the Handling Arrangements now in force cannot recur (and if such policy were to change it would be publicly avowed and new Arrangements would be published), this confirmation by the Respondents applies not only to the present but also to the period since 2010. The Respondents have further confirmed that the SIAs have not threatened the use of such compulsory powers in obtaining the BPDs that they hold and/or have held in such period. Hence there is no issue to be referred in respect of BPD.

6. The context of the issues before us has been as to the balance between the steps taken by the State, through the SIAs, to protect its population against terror and threat to life against the protection of privacy of the individual. Subject to the reservation of the issues referred to in paragraph 1 above, we were and are satisfied that the BCD and BPD regimes complied with the ECHR. We now need to consider whether EU law, particularly by reference to the Charter of Fundamental Rights of the European Union (2000/C364/01)

("the Charter") adopted by the European Union on 1 December 2009, by amendment of Article 6(1) of the Treaty on European Union ("TEU"), applies, and, if so, imposes a higher, and the Respondents submit, impossible and inappropriate, standard as a result of, or by reference to, **Watson**.

7. We set out the following in paragraph 21 of our October Judgment. The emphasis is only underlined by the continued and increasing series of deplorable attacks on civilians in London and Manchester.

> "*It is important to emphasise that the Tribunal and the parties recognise that there is a serious threat to public safety, particularly from international terrorism, and that the SIAs are dedicated to discharging their responsibility to protect the public. It is understandable in the circumstances that the Respondents, both through Mr. Eadie orally and by their evidence, have emphasised the important part which the use of BCD and BPD have played in furthering that protection, particularly where those who pose the threat are using increasingly sophisticated methods to protect their communications. In a Report published on 19th August 2016 (the "Bulk Powers Review") David Anderson QC, the Independent Reviewer of Terrorism Legislation, concluded that there is a proven operational case for the use of the powers to obtain and use BCD and BPD, that those powers are used across the range of activities of the SIA, from cyber-security, counter-espionage and counter-terrorism to child sexual abuse and organised crime, and that such powers play an important part in identifying, understanding and averting threats to Great Britain, Northern Ireland and elsewhere.*"

We shall refer further to that Bulk Powers Review by Mr Anderson QC, the then Independent Reviewer of Terrorism Legislation, (which we shall call "the Anderson Report") below.

8. So far as BCD is concerned, its acquisition by the SIAs is described in paragraph 22 and following of the October Judgment, namely by virtue of directions issued by the Secretary of State, pursuant to s.94 to

telecommunications providers ("PECNs") to supply communications data (but not content) to MI5 and to GCHQ. S. 94 reads, in relevant part, as follows:

> "*(1) The Secretary of State may, after consultation with a person to whom this section applies, give that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.*
>
> *(2) If it appears to the Secretary of State to be necessary to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom the section applies, give to that person a direction requiring him (according to the circumstances of the case) to do or not to do , a particular thing specified in the direction.*
>
> *(2A) The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct."*

9. The Respondents put forward in the course of the hearing before us what Mr Eadie QC called four key factual propositions. As to the first two, Mr de la Mare QC for the Claimant did not, subject to questions of proportionality, take issue at the hearing or regard them as "*especially controversial*". They were:

i) The use of Bulk Data capabilities is critical to the ability of the SIAs to secure national security;

ii) A fundamental feature of many of the SIAs' techniques of interrogating Bulk Data is that they are non-targeted, i.e. not directed at specific targets. Clarification in this regard is given on page 32 of the 2015 report by the Intelligence & Security Committee of Parliament ("ISC"):

> "*It is essential that the Agencies can "discover" unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on "known" threats: Bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats.*"

10. In relation to the third and fourth of Mr Eadie's propositions there is however acute dispute:

iii) That the existing safeguards [found to be compliant (with the reservations set out in paragraph 2 above) with the ECHR in our October Judgment] are sufficient to prevent abuse in connection with the SIAs' use of the capabilities derived from BCD/BPD;

iv) That if applied to the field of national security, the requirements specified by the Grand Chamber in **Watson** ("the Watson Requirements") would effectively cripple the SIAs' Bulk Data capabilities.

The Facts

11. The Respondents have put in a good deal of evidence (including written statements which refer to case studies), to which we shall refer further below.

The importance however of the Anderson Report, which evaluated the operational case for the use (inter alia) of BCD, is that it was conducted by a team of independent persons (described in paragraph 1.32 of the Report), with considerable expertise in the use of secret intelligence, and with the necessary security clearance to obtain access to secret documents, in order to analyse a number of actual case studies, to judge the effect and utility of the bulk powers. The reviewers were not only able to review documents, but also to question intelligence officers to ascertain whether the case being made for the use of those powers was justified.

12. Included in the Anderson Report case studies were two which illustrated the necessity for access to Bulk Data following terrorist attacks carried out by persons who were not under surveillance, which has been the case in a number of recent terrorist attacks in the United Kingdom. The findings of those two case studies are set out below:

> "***Case study A9/10***
>
> *This case study related to the London and Glasgow attacks in 2007. Using bulk acquisition data, MI5 was able to establish within hours that the same perpetrators were responsible for both attacks. MI5 was also able, within a similarly short period, to learn more about the details of the attacks, including the methods used and the identities of those involved or associated with the attackers. The ability to conduct this analysis at pace enabled MI5 to support the police in responding swiftly to the attacks and to the threat of further, imminent attacks.*
>
> *It would not have been possible to achieve the same results with comparable speed, using targeted queries. Speed was essential at the time, when the SIAs and police had to learn as quickly as possible whether other attacks were imminent. Bilal Abdulla was subsequently convicted of conspiracy to murder and conspiracy to cause explosions likely to endanger life. Kafeel Ahmed died of the injuries that he sustained at Glasgow Airport, having set himself alight.*

Case study A9/11

In 2010, a network of terrorists – comprising groups in Cardiff, London and Stoke-on-Trent - planned a series of bomb attacks at several symbolic locations in the UK, including the London Stock Exchange. Complex analysis of bulk acquisition data played a key role in identifying the network. The task was made particularly challenging by the geographical separation of the groups. Nine members of the network were subsequently charged and pleaded guilty to terrorism offences relating to the plot. Eight members of the network pleaded guilty to engaging in conduct in preparation for acts of terrorism.

MI5 reiterated to the Review team the assertion it had already made in public that the use of targeted communications data would not have allowed it to identify the attackers and understand the links between them with the speed made possible by the use of bulk acquisition data."

There are several other similar case studies in Annex 9 of the Anderson Report. As the Report noted (at paragraph 2.33) it is an important and distinctive feature of the SIAs' current capability that data obtained pursuant to s.94 can be aggregated in one place.

13. The overall conclusion of Mr Anderson QC, at paragraph 6.47, was as follows:

"*I have concluded that:*

(a) *Bulk acquisition has been demonstrated to be crucial in a variety of fields, including counter-terrorism, counter-espionage and counter-proliferation. The case studies provide examples in which bulk acquisition has contributed significantly to the disruption of terrorist operations and, through that disruption, almost certainly the saving of lives.*

(b) *Bulk acquisition is valuable as a basis for action in the face of imminent threat, though its principal utility lies in swift target identification and development.*

(c) *The SIAs' ability to interrogate the aggregated data obtained through bulk acquisition cannot, at least with currently available technology, be matched through the use of data obtained by targeted means.*

> *(d) Even where alternatives might be available, they are frequently more intrusive than the use of bulk acquisition.*"

14. Those findings fully support the evidence given in this case by the Respondents that the use of bulk communications data is of critical value to the intelligence agencies, and is of particular value in identifying potential threats by persons who are not the target of any investigation. These datasets need to be as comprehensive as possible if they are to be effective. The use of these datasets is very different from, for example, their use in an investigation of a criminal offence by police, in which case the police may well have an identified suspect who can be made the subject of a targeted investigation. The Respondents' witnesses speak persuasively of developing fragmentary intelligence, of enriching 'seed' information, of following patterns and anomalies, and of the need for the haystack in order to find the needle.

15. The MI5 witness concluded his statement as follows:

> "*152) In my capacity as Deputy Director for Data Access and Policy I saw how vital BCD is for the work of MI5, in particular in relation to counter-terrorism work. I am able to say, based on what I have seen myself and been told by colleagues in MI5, that the use of BCD by MI5 has stopped terrorist attacks and has saved lives many times.*
>
> *153) The acquisition of BCD enables MI5 to identify threats and investigate in ways that, without this capability, would be either impossible or considerably slower. In many case*[s] *communications data may be the only investigative lead that we have to work from. Further, without BCD, it would be necessary to carry out other and more intrusive enquiries; for example many more individual requests for CD or use other more intrusive powers in order to narrow the scope of a search. The inability to use BCD would therefore involve greater intrusion into the privacy of individuals.*

> *154) I recognise of course that, simply by holding BCD that relates to individuals who are not of intelligence interest, and as with BPD, there is a degree of interference with the privacy of such individuals. However, the BCD in the database is, itself, anonymous. Further, and as with all bulk capabilities, whilst it is right to acknowledge that a significant quantity of information can be collected, only a tiny proportion of the data is ever examined.*"

In paragraph 9.14(b) of the Anderson Report, the conclusion is recorded that for MI5 the bulk acquisition power "*has contributed significantly to the disruption of terrorist operations and the saving of lives*".

16. The evidence contained in the Anderson Report does not completely resolve the question of proportionality, which issue has not yet been determined by this Tribunal, but it does very clearly establish the purpose for which these powers are deployed and how they are used. They are used not to access, still less to examine, the personal data of all those contained within the dataset, but, to the contrary, by a process of elimination, and with minimal intrusion, to obtain access only to the data of persons whose activities may constitute a threat to national security. That point was illustrated in the evidence, giving an example of how in 2005, on the basis of sensitive but fragmentary intelligence, it was possible for MI5, from an entire BPD dataset, to establish, by applying a number of filters and matches so as to reduce a pool of 27,000 candidates, one person who was identified as a suspected potential Al-Qaeda suicide bomber.

17. Nothing in the evidence and materials we have seen contradicts what is set out in paragraphs 11 to 16 above, and we accept it. The finding of this Tribunal is

that these capabilities are essential to the protection of the national security of the United Kingdom.

The disputed impact of **Watson**

18. It is in this context that we turn to consider the issue before us as to the impact of the Grand Chamber's decision in **Watson** upon the conclusions we have reached as to the proper balance, by reference to the ECHR, between privacy of the individual and protection of the public, against the background of the ever-increasing threats to national security, summarised in the evidence before us and in any event well known.

19. The s.94 regime is unlike the provisions of the Data Retention and Investigatory Powers Act 2014 ("DRIPA"), which was the Act considered in **Watson**, whereby a public telecommunications operator, or provider, could be required by the Secretary of State, by a retention notice, to retain commercial data longer than their commercial needs required, so as to be available to the SIAs as and when called upon. S.94 requires communications data to be delivered up to the SIAs, so as to constitute BCD in their custody. Access is then either for a targeted purpose or, more likely, there is an electronic trawling of masses of data, which are not themselves read, in order to discover, as referred to above, the needle in the haystack. A miniscule quantity of the data trawled is ever examined. There is thus no genuine intrusion to any save that miniscule proportion.

20. The Claimant submits that, in the light of **Watson**, the acquisition (and access to and use of) BCD is unlawful at EU law. The Respondents however submit that no such conclusion can be reached, in that:

i) the conclusions of the Grand Chamber in **Watson** in respect of DRIPA have no effect, even by extension or analogy, upon BCD acquired and used for the purposes of national security, which requires separate consideration:

ii) if it were of application to matters of national security, the **Watson** judgment would not comply with the TEU, as being inconsistent with the provisions of TEU Articles 4 and 5 (set out below), and with previous decisions of the Grand Chamber.

iii) the safeguards of ECHR Article 8 are sufficient to control the activities of the States and the SIAs, and achieve a sufficient balance between the protection of the public and the privacy of the individual, and the Watson Requirements do not or should not apply to BCD.

EU Law

21. The relevant EU provisions are as follows:

i) TEU/TFEU

Article 4 TEU

> "*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.*
>
> . . ."

Article 5 TEU

"*1. The limits of Union competences are governed by the principle of conferral. . . .*

2. Under the principle of conferral the Union shall act only within the limits of the competences conferred upon it by the Member State in the Treaties to obtain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member State.

. . ."

Article 6 TEU

"*1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which will have the same legal value as the Treaties.*

The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties.

The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions entitled VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.

2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.

3. Fundamental rights, as guaranteed by the European Convention . . . and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's as law."

Article 16 TFEU

"*1. Everyone has the right to the protection of personal data concerning them.*

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law,

and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

. . ."

ii) The Charter

Article 7: Respect for Private and Family Life

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

Article 8: Protection of Personal Data

"*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."

Article 51: Scope

"*1. The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union Law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers.*

2. This Charter does not establish any new power or task for the Community or the Union, or modify powers and tasks defined by the Treaties."

iii) The Data Protection Directive ("DPD") 95/46 EC

Recital 13:

"*Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States*

under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters."

Article 3

"*Scope*

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

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

- by a natural person in the course of a purely personal or household activity."

iv) The E Privacy Directive ("EPD") 2002/58 EC

Recital 11

"*Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by*

the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms."

Article 1

"*Scope and aim*

1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. 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."

Article 15

"*Application of certain provisions of Directive 95/46/EC*

1. *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.

. . ."

22. There were two important decisions of the Grand Chamber in particular, prior to **Watson**:

i) **The European Parliament v Council of the European Union** ("**Parliament v Council**") [2006] 3 CMLR 9. This is relied upon by the Respondents, and was not addressed in **Watson**. It concerned the supply of passenger data ("PNR data") by air carriers to the US Authorities. The Court upheld the arguments of the Council that Article 3(2) of the DPD (set out above), which excluded activities to safeguard national security as falling outside the scope of Community Law, was infringed:

> "*56. It follows that the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the state in areas of criminal law.*
>
> *57. While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community Law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision on adequacy is, however, quite different in nature. As pointed out in para. [55] of the present judgment, that decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes.*
>
> *58. The court held in para. [43] of **Lindqvist**, which was relied upon by the Commission in its defence, that the activities mentioned by way of example in the first indent of Art.3(2) of the Directive are, in any event, activities of the state or of state authorities and unrelated to the fields of activity of individuals. However, this does not mean that, because the PNR*

data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country, the transfer in question is not covered by that provision. The transfer falls within a framework established by the public authorities that relates to public security.

59. It follows from the foregoing considerations that the decision on adequacy concerns processing of personal data as referred to in the first indent of Art.3(2) of the Directive. That decision therefore does not fall within the scope of the Directive."

ii) **Digital Rights Ireland Ltd v Communications Minister** [2015] QB 127 ("**DRI**"). This was adopted and applied by the Grand Chamber in **Watson**. **DRI** related to provisions in the then Data Retention Directive 2006/24/EC ("the DRD"), which required PECNs to ensure the retention of personal data for the purpose of fighting serious crime, and found them to be in breach of Articles 7 and 8 of the Charter, and consequently invalid. DRIPA, the statute passed by the UK legislature (but with a 'sunset clause' expiring at the end of 2016) to replace the DRD, which was the subject (together with a Swedish statute) of **Watson**, was obviously very analogous. The Court in **DRI** laid down requirements in relation to the data so retained by the operators which formed the basis of the Watson Requirements.

Watson

23. The first of the two conjoined cases in **Watson** related to a Swedish statute which authorised the collection of data, in the context of criminal offences punishable by a term of imprisonment of 2 years, or in some cases less. DRIPA, as described in paragraph 19 above, provided for a retention notice requiring PECNs to retain communications data if the Secretary of State considered it necessary and proportionate for one or more of the purposes

contained in S.22(2) of the Regulation of Investigatory Powers Act 2000 ("RIPA"). It is clear that (save for the short passage in one paragraph of the Judgment, 119), the conclusion by the Grand Chamber in **Watson** was reached by reference to the investigation of crime, not national security; and the Court in any event made clear (paragraph 115) that it was only serious crime (i.e. not such crime as was within the remit of the Swedish statute) which could justify access to such retained data. S.94, as made clear in the October Judgment, and as set out in paragraph 19 above, relates to the directions by the Secretary of State to PECNs to supply BCD to GCHQ and MI5 (not retain it themselves), as necessary and proportionate in the interests of national security (or of relations with foreign governments).

24. The **Watson** judgment falls primarily into two parts. The first consists of consideration of the scope of the EPD, addressing the Swedish statute and then DRIPA.

25. As to this part, the consideration of the scope of the EPD commences in paragraph 65 of the Judgment, and in paragraphs 68 to 71 refers to Article 1 of the EPD, and in particular Article 1(3), noting that it excluded from the scope of the Directive "*the activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters.*" Reference is made to judgments of the European Court, not including **Parliament v Council**. Paragraph 70 refers to Article 3 of the EPD, which states that the Directive does apply to the processing of personal data by providers of electronic communication services, and paragraph 71 then refers

to Article 15(1), whereby Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in the relevant Articles, including measures providing for the retention of data. The Judgment then continues in paragraphs 72 to 81 to conclude that the legislative measures contained in the Swedish statute and in DRIPA fell within the scope of the EPD, notwithstanding Article 1(3). There is no mention of Article 4 of the TEU set out in paragraph 21 above, but there is a construction/interpretation of Article 15 of the EPD in the context of Article 1(3):

> "*72. Admittedly, the legislative measures that are referred to in Article 15(1) of Directive 2002/58 concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active (see, to that effect, judgment of 29 January 2008,* ***Promusicae****, C-275/06, EU:C:2008:54, paragraph 51). Moreover, the objectives which, under that provision, such measures must pursue, such as safeguarding national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that directive.*
>
> *73. However, having regard to the general structure of Directive 2002/58, the factors identified in the preceding paragraph of this judgment do not permit the conclusion that the legislative measures referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, 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.*
>
> *74. Further, the legislative measures referred to in Article 15(1) of Directive 2002/58 govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services. Accordingly, Article 15(1),*

read together with Article 3 of that directive, must be interpreted as meaning that such legislative measures fall within the scope of that directive.

75. The scope of that directive extends, in particular, to a legislative measure, such as that at issue in the main proceedings, that requires such providers to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data.

76. The scope of that directive also extends to a legislative measure relating, as in the main proceedings, to the access of the national authorities to the data retained by the providers of electronic communications services.

77. The protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including 'any data related to such communications', in order to protect the confidentiality of electronic communications.

78. In those circumstances, a legislative measure whereby a Member State, on the basis of Article 15(1) of Directive 2002/58, requires providers of electronic communications services, for the purposes set out in that provision, to grant national authorities, on the conditions laid down in such a measure, access to the data retained by those providers, concerns the processing of personal data by those providers, and that processing falls within the scope of that directive.

79. Further, since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services.

80. That interpretation is confirmed by Article 15(1b) of Directive 2002/58, which provides that providers are to establish internal procedures for responding to requests for access to users' personal data, based on provisions of national law adopted pursuant to Article 15(1) of that directive.

81. It follows from the foregoing that national legislation, such as that at issue in the main proceedings in Cases C-203/15 and C-698/15, falls within the scope of Directive 2002/58."

26. The second part of the Judgment, headed "*The interpretation of Article 15(1) of [EPD] in the light of Articles 7, 8, 11 and Article 52(1) of the Charter*", primarily in paragraph 89 onwards addresses the two relevant statutes, by reference to targeted access to data for the purpose of combating crime:

> "*89. Nonetheless, in so far as Article 15(1) of Directive 2002/58 enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data, that provision must, in accordance with the Court's settled case-law, be interpreted strictly (see, by analogy, judgment of 22 November 2012,* ***Probst****, C-119/12, EU:C:2012:748, paragraph 23). That provision cannot, therefore, permit the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58, to become the rule, if the latter provision is not to be rendered largely meaningless.*
>
> *90. 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 (see, to that effect, judgment of 29 January 2008,* ***Promusicae****, C-275/06, EU:C:2008:54, paragraph 53). That list of objectives is exhaustive, as is apparent from the second sentence of Article 15(1) of Directive 2002/58, which states that the legislative measures must be justified on 'the grounds laid down' in the first sentence of Article 15(1) of that directive. Accordingly, the Member States cannot adopt such measures for purposes other than those listed in that latter provision.*
>
> *91. Further, the third sentence of Article 15(1) of Directive 2002/58 provides that '[a]ll the measures referred to [in Article 15(1)] shall be in accordance with the general principles of [European Union] law, including those referred to in Article 6(1) and (2) [EU]', which include the general principles and fundamental rights now guaranteed by the Charter. Article 15(1) of Directive 2002/58 must, therefore, be interpreted in the light of the fundamental rights guaranteed by*

*the Charter (see, by analogy, in relation to Directive 95/46, judgments of 20 May 2003, **Österreichischer Rundfunk and Others**, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; of 13 May 2014, **Google Spain and Google**, C-131/12, EU:C:2014:317, paragraph 68, and of 6 October 2015, **Schrems**, C-362/14, EU:C:2015:650, paragraph 38).*

*92. In that regard, it must be emphasised that the obligation imposed on providers of electronic communications services, by national legislation such as that at issue in the main proceedings, to retain traffic data in order, when necessary, to make that data available to the competent national authorities, raises questions relating to compatibility not only with Articles 7 and 8 of the Charter, which are expressly referred to in the questions referred for a preliminary ruling, but also with the freedom of expression guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the **Digital Rights** judgment, paragraphs 25 and 70).*

*93. Accordingly, the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 of the Charter, as derived from the Court's case-law (see, to that effect, judgment of 6 October 2015, **Schrems**, C-362/14, EU:C:2015:650, paragraph 39 and the case-law cited), must be taken into consideration in interpreting Article 15(1) of Directive 2002/58. The same is true of the right to freedom of expression in the light of the particular importance accorded to that freedom in any democratic society. That fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (see, to that effect, judgments of 12 June 2003, **Schmidberger**, C-112/00, EU:C:2003:333, paragraph 79, and of 6 September 2011, **Patriciello**, C-163/10, EU:C:2011:543, paragraph 31).*

94. In that regard, it must be recalled that, under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (judgment of 15 February 2016, N., C-601/15 PPU, EU:C:2016:84, paragraph 50).

> *95. With respect to that last issue, the first sentence of Article 15(1) of Directive 2002/58 provides that Member States may adopt a measure that derogates from the principle of confidentiality of communications and related traffic data where it is a 'necessary, appropriate and proportionate measure within a democratic society', in view of the objectives laid down in that provision. As regards recital 11 of that directive, it states that a measure of that kind must be 'strictly' proportionate to the intended purpose. In relation to, in particular, the retention of data, the requirement laid down in the second sentence of Article 15(1) of that directive is that data should be retained 'for a limited period' and be 'justified' by reference to one of the objectives stated in the first sentence of Article 15(1) of that directive.*
>
> *96. Due regard to the principle of proportionality also derives from the Court's settled case-law to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary (judgments of 16 December 2008,* ***Satakunnan Markkinapörssi and Satamedia****, C-73/07, EU:C:2008:727, paragraph 56; of 9 November 2010,* ***Volker und Markus Schecke and Eifert****, C-92/09 and C-93/09, EU:C:2010:662, paragraph 77; the* ***Digital Rights*** *judgment, paragraph 52, and of 6 October 2015,* ***Schrems****, C-362/14, EU:C:2015:650, paragraph 92).*"

27. In paragraph 97 to 107, the Court primarily addresses the Swedish statute and is critical of it, citing a number of paragraphs of the **DRI** Judgment, and concludes in respect of the First Question (raised in the Swedish proceedings), against the background of the Swedish statute and the context of investigation of crime, as follows:

> "*108. However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.*
>
> *109. In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national*

legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the ***Digital Rights*** *judgment, paragraph 54 and the case-law cited).*

110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111. 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. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.

112. Having regard to all of the foregoing, the answer to the first question referred in Case C-203/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication."

28. After discussion by the Court of both statutes in the light of its conclusions on the scope of the Directive, the part of its Judgment containing the Watson Requirements is in paragraphs 119 to 125:

> "*119. Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, 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 (see, by analogy, ECtHR, 4 December 2015,**Zakharov v. Russia**, CE:ECHR:2015:1204JUD0047143 06, § 260). 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.*
>
> *120. In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, the **Digital Rights** judgment, paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016, **Szabó and Vissy v. Hungary**, CE:ECHR:2016:0112JUD0037 13814, §§ 77 and 80).*
>
> *121. Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly*

*provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, judgments of 7 May 2009, **Rijkeboer,** C-553/07, EU:C:2009:293, paragraph 52, and of 6 October 2015, **Schrems**, C-362/14, EU:C:2015:650, paragraph 95).*

*122. With respect to the rules relating to the security and protection of data retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the **Digital Rights** judgment, paragraphs 66 to 68).*

*123. In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (see, to that effect, the **Digital Rights** judgment, paragraph 68, and the judgment of 6 October 2015, **Schrems**, C-362/14, EU:C:2015:650, paragraphs 41 and 58).*

124. It is the task of the referring courts to determine whether and to what extent the national legislation at issue in the main proceedings satisfies the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as set out in paragraphs 115 to 123 of this judgment, with respect to both

the access of the competent national authorities to the retained data and the protection and level of security of that data.

125. Having regard to all of the foregoing, the answer to the second question in Case C-203/15 and to the first question in Case C-698/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, 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."

Scope

29. The Respondents' stance in this application starts from the relatively uncontentious position that:

i) As summarised in paragraphs 19 and 23 above, DRIPA was a different statute, and related to the retention by providers of communications data beyond their commercial needs, so as to be available for access by the SIAs. S.94 relates to the supply of BCD to the SIAs via the providers, who do not thereafter retain the data (beyond the period of their requirements), which is retained by the State (the SIAs). The Judgment emphasises in paragraphs 70, 78-80 and 92 the obligations of the providers.

ii) The judgment in **Watson** was addressing the targeted access of data in criminal investigations. Paragraph 106 of the **Watson** judgment refers to and adopts paragraph 59 of the **DRI** judgment, which emphasises as objectionable the lack of any need for a specified relationship between the data sought and any identified particular persons or group. This falls to be contrasted with the

needs of national security, as particularly exemplified in the passage from the ISC Report set out in paragraph 9(ii) above.

30. However, much more significantly, the Respondents point out that the Grand Chamber in **Watson** did not deal with Article 4(2) of the TEU and the consequence of the exclusion of (in particular) national security from the ambit of the Treaty. The Respondents submit that the Member States have the *sole responsibility* (Article 4(2)) for national security, that the Charter does not apply (Article 6 of the TEU and Article 51 of the Charter), and that the case is on all fours with the Court's decision in **Parliament v Council**, in which the supply of PNR data by the parties to the US Authorities for public security purposes was "*within a framework established by the public authorities that relates to public security*" and "*does not fall within the scope of the Directive*" (paragraph 58-59 of the Judgment). The Respondents submit that the Charter is of no relevance, and that the BCD regime should be tested only against the requirements of the ECHR.

31. We shall for the moment leave aside the asserted distinguishing features referred to in paragraph 29 above, which become particularly significant in our consideration of the application or relevance of the Watson Requirements, though they must obviously be borne in mind when and if the Grand Chamber comes to consider or reconsider in this national security context whether the EPD applies at all. The Respondents accept that, even though all that the providers do pursuant to a s.94 direction is supply data, that does involve them in taking steps which would constitute processing of personal data within the

meaning of Article 1 of the EPD, but it would be, as they assert, an activity outside the scope of the Treaty, by virtue of Article 1(3) of the EPD.

32. As set out in paragraph 30 above, the Respondents' case is based upon Articles 4 and 5 of the TEU. The Union's legal competence is governed by the principle of conferral (Article 5). By Article 4(2) the Member States, whose sole responsibility it remains, have not conferred the *essential State functions* of national security on the Union. Hence by Article 16(2) TFEU the European Parliament and Council have only the power to lay down rules relating to the processing of personal data in relation to activities which fall within the scope of EU law, as Article 1(3) of the EPD itself records (as does Article 3(2) of the DPD). By Article 6 of TEU, the provisions of the Charter do not extend the competences of the Union, and by Article 51 of the Charter its provisions only apply to the Member States when they are implementing Union Law. Consequently the activities of the Member States in relation to national security, by way of requiring the supply of BCD and thereafter accessing and using it, are not derogations from the Member States' obligations under the Treaty, requiring strict construction and limitation, but are outside the jurisdictional limit of the Treaty's competence, and for the Union to interfere consequently impacts on the sovereignty of the Member State, and is likely to have the potential consequence that it cannot comply with Treaty obligations with other countries e.g. for the sharing of intelligence. The **Watson** Requirements plainly lay down conditions to be applied to Member States e.g. at paragraphs 118 and 125, which, if applied in the national security context, the Respondents assert to be matters outside the jurisdiction of the Union.

33. The Respondents point to **Parliament v Council**, to which we have referred in paragraphs 22(i) and 30 above, which appears to be a judgment on all fours with this case and to point to the opposite conclusion than that reached by the Grand Chamber in **Watson**. As set out above, the processing operations in question in that case consisted (paragraph 56) of the transfer of PNR data to the United States Department of Customs Border Protection ("CBP") which constituted "*processing operations concerning public security*", and hence within Article 3(2) and outside the ambit of the DPD (and consequently also the EPD). Mr de la Mare for the Claimant sought to explain the decision by asserting that the data supplied were not required by the carriers for their commercial purposes, i.e. that they had data which was required for their commercial purposes, which they retained and did not supply, and also had data which was not required for their commercial purposes, which they did supply, hence outside the DPD/EPD. But it is clear that this is not a correct analysis, and is a misreading of paragraph 57 of the Judgment, and in particular the last sentence. It is not arguable, because the PNR data, which are fully described in paragraph 27 of the Judgment, did plainly include data required by the carriers for their commercial purposes. After recording, at paragraph 55, the fact that the decision concerned PNR data transferred to CBP, the Grand Chamber states, in paragraph 57, that its decision concerned (our underlining) "*not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security*". What the Court is plainly stating is that in relation to data, all of which was required for the carriers' commercial purposes, the data processing required for the supply to CBP was processing required not for the supply of services

but for public security purposes. The decision was not in relation to the data but the processing. This is made clear, and indeed was adopted, by the Grand Chamber in paragraph 88 of **Ireland v European Parliament** [2009] 2 CMLR 37 (the "*latter decision*" referred to is **Parliament v Council**):

> "*88. The latter decision concerned the transfer of passenger data from the reservation systems of air carriers situated in the territory of the Member States to the United States Department of Homeland Security, Bureau of Customs and Border Protection. The Court held that that the subject matter of that decision was data-processing which was not necessary for a supply of services by the air carriers, but which was regarded as necessary for safeguarding public security and for law-enforcement purposes. At [57] to [59] of the judgment in* ***Parliament v Council****, the Court held that such data processing was covered by art.3(2) of Directive 95/46, according to which that Directive does not apply, in particular, to the processing of personal data relating to public security and the activities of the state in areas of criminal law. The Court accordingly concluded that Decision 2004/535 did not fall within the scope of Directive 95/46.*
>
> . . .
>
> *91. Unlike Decision 2004/496 which concerned a transfer of personal data within a framework instituted by the public authorities in order to ensure public security, Directive 2006/24 covers the activities of service providers in the internal market and does not contain any rules governing the activities of public authorities for law-enforcement purposes.*"

34. Accordingly, **Parliament v Council** is of direct significance. Notwithstanding that the processing and transfer of data addressed in that case was effected by commercial undertakings, whose activities were subject to the DPD, the Grand Chamber held that the processing of such data was in the course of an activity which fell outside the scope of Community law, as provided for by Article 3(2). As appears in paragraph 20(i) above, the Court held, at paragraph 57, that the processing was different in nature from an activity which fell within the scope of Community law and, at paragraph 58, that the transfer of data fell

within a framework established by the public authorities that related to public security. On that point the Court followed the decision in **Criminal Proceedings against Lindqvist [C-101/01)** at paragraph 43, that activities of the state or state authorities concerning public and state security were in any event unrelated to the activities of individuals or, it seems commercial undertakings, whose activities would be governed by the Directives.

35. This exclusion of certain activities from the jurisdiction of the Union is clearly explained in **Remondis GmbH & Co. KG Region Nord v Region Hannover** (Case C-51/15, 21 December 2016), in relation to an activity which was excluded by Article 4(2) of the TEU, namely the organisation of local government. Mengozzi AG in his Opinion of 30 June 2016 stated as follows:

> "*38. It is nevertheless clear from the case-law that the internal organisation of the State does not fall under EU law. The Court has recognised on several occasions that each Member State is free to delegate powers internally as it sees fit (24) and that the question of how the exercise of public powers is organised within the State is solely a matter for the constitutional system of each Member State.*
>
> . . .
>
> *41. As acts of secondary legislation, such as Directive 2004/18 in this case, must be in conformity with primary law, such acts cannot be interpreted as permitting interference in the institutional structure of the Member States. Accordingly, acts of internal reorganisation of the powers of the State remain outside the scope of EU law and, more specifically, EU rules on public procurement.*
>
> *42. An act by which a public authority, unilaterally in the context of its institutional powers, or several public authorities, in the context of an agreement governed by public law, make a transfer of certain public powers from one public entity to another public entity constitutes an act of internal reorganisation of the Member State. Such an act therefore, in principle, falls outside the scope of EU law and, more specifically, the EU rules on public procurement.*"

This was approved by the Court at paragraphs 41 and 42:

> "*41. Moreover, as that division of competences is not fixed, the protection conferred by Article 4(2) TEU also concerns internal reorganisations of powers within a Member State, as observed by the Advocate General in points 41 and 42 of his Opinion. Such reorganisations, which may take the form of reallocations of competences from one public authority to another imposed by a higher-ranking authority or voluntary transfers of competences between public authorities, have the consequence that a previously competent authority is released from or relinquishes the obligation or power to perform a given public task, whereas another authority is henceforth entrusted with that obligation or power.*
>
> *42. Secondly, such a reallocation or transfer of competence does not meet all of the conditions required to come within the definition of public contract.*"

36. The Respondents also refer to:

i) Mengozzi AG's Opinion of 8 September 2016 1/15, in which he refers to ***Parliament v Council***:

> "*85. The Court was asked by the Parliament to determine, in particular, whether the Commission was authorised to adopt an adequacy decision, based on Article 25 of Directive 95/46 on the adequate protection of personal data contained in the Passenger name Record of air passengers transferred to the United States, when Article 3(2) of that directive expressly excluded from its scope processing operations concerning, in particular, public security and the activities of the State in areas of criminal law. The Court logically replied in the negative. In fact, the processing of the PNR data in the context of the agreement with the United States could not be associated with the supply of services, but fell within a framework established by the public authorities that related to public security, which did not come within the scope of Directive 95/46.*"

ii) The European Council Notice 2016/C691/01 of February 2016. This was a statement made by the European Council in the context of a hoped for new

settlement for the UK within the European Union, which did not take place, but it constituted a statement of the existing law, in Section C (Sovereignty):

> "*5. Article 4(2) of the Treaty on European Union confirms that national security remains the sole responsibility of each Member State. This does not constitute a derogation from Union law and should therefore not be interpreted restrictively. In exercising their powers, the Union institutions will fully respect the national security responsibility of the Member States.*"

Mr Eadie submits that this can be relied upon pursuant to Article 31 of the Vienna Convention on the Law of Treaties 1969.

37. As set out above, the Grand Chamber in **Watson** did not refer to any of the matters set out in paragraphs 32 to 36 above. It did however record, in paragraphs 69 and 72 of the Judgment, Article 1(3) of the EPD. It considered that there was an apparent conflict (or "*overlap*") between Article 1(3) and Article 15 of the EPD, and considered that Article 15 would be "*deprived of any purpose*" if it was not to be read, despite Article 1(3), as "*meaning that such legislative measures fell within the scope*" of the EPD. This would appear to have the consequence that:

i) It would be Article 1(3) that would thus be "*deprived of any purpose*";

ii) Effect would thus not be given to Article 4 of TEU; and/or

iii) Contrary to EU law, Article 4, a primary provision of the Treaty, would be replaced/contravened by secondary legislation, namely Article 15 of the Directive, notwithstanding Article 1(3).

38. The Claimant's first response to this can be summarised by Mr de la Mare's statement that national security should not be seen as a 'magic lamp'. The way he put it in argument was that once you choose to have an exception, which is used to derogate from or qualify the rights and obligations in Article 5 of EPD, that must conform with the minimum standards supplied by EU law. Effectively this was a statement that national security does not constitute an ouster of jurisdiction, or a framework outside the Treaty, but a derogation (contrary to the Statement in paragraph 36(ii) above, and the Respondents' submissions in paragraph 32 above).

39. He submits that the words in Article 4 TEU, that the Union must respect essential State functions including safeguarding national security, and in particular that national security remains the '*sole responsibility*' of each Member State, must be read so as to mean that *sole responsibility* should be read as sole administrative or executive responsibility. Thus he submits that the kinds of activities which are outside the scope of the Treaty or a Directive by virtue of Article 4 are decisions as to the resources of GCHQ or its staffing, or the location of its headquarters, or, he suggested, activities such as the running by the Ministry of Defence of its own telecommunications network, being outside the ambit of the Directive, or the allocation internally between its agencies of the responsibility for counter-terrorism. This does not seem to us to be very persuasive. The suggested watering down of *sole responsibility* does not ring true against the principle of conferral set out in Article 5, and the suggested activities said to remain within the *sole responsibility* appear to be trifling.

40. He submits in any event that the activities of the security services of Member States are outside the scope of the TEU only insofar as they do not disturb the rights and obligations imposed by EU law, the corollary of which is that the EU has no competence to undertake work to further the national security of any Member State, and cannot comment on the adequacy or inadequacy of any Member State's efforts, or demand any particular steps be taken in that regard. He points out that national security has not amounted to a 'get out' in the context of freedom of movement or goods (notwithstanding the express exclusions for national security in Articles 36 and 52 of TFEU). Thus in **European Commission v Italian Republic** Case C-*387*/05 judgment of 15 December 2009 the Court stated:

> "*45. According to the Court's settled case-law, although it is for Member States to take the appropriate measures to ensure their internal and external security, it does not follow that such measures are entirely outside the scope of Community law (see Case C-273/97* ***Sirdar*** *[1999] ECR I-7403, paragraph 15, and Case C-285/98* ***Kreil*** *[2000] ECR I-69, paragraph 15). As the Court has already held, the only articles in which the Treaty expressly provides for derogations applicable in situations which may affect public safety are Articles 30 EC, 39 EC, 46 EC, 58 EC, 64 EC, 296 EC and 297 EC, which deal with exceptional and clearly defined cases. It cannot be inferred that the Treaty contains an inherent general exception excluding all measures taken for reasons of public security from the scope of Community law.*"

41. This was followed by the Grand Chamber in **ZZ (France) v Secretary of State for the Home Department** Case C-300/11 [2013] QB 1136, a case which considered whether an individual facing expulsion from the UK was entitled to a gist of the case against him in the Special Immigration Appeal Commission. The Court said in paragraph 38:

> "*Furthermore, although it is for member states to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns state security cannot result in European Union law being inapplicable.*"

Mr de la Mare points out that when **ZZ** was returned to the Court of Appeal, [2004] QB 820, Richards LJ stated at paragraph 18 that the gist was a "*minimum requirement which cannot yield to the demands of national security*", and continued "*nor is there anything particularly surprising about such a result in the context of restrictions on the fundamental rights of free movement and residence of Union citizens under European Union law*". Mr de la Mare also points to the role of EU law in the pre-Human Rights Act cases of **R v Secretary of State for the Home Department ex p Gallagher** [1995] ECR I-4253 and **R (Shingara and Radiom) v Secretary of State for the Home Department** [1997] ECR I-3343, where Articles 8 and 9 of Council Directive 64/221EEC were applied without challenge, in cases of national security.

42. The Claimant submits that **Watson** is binding and should be followed, even though the facts are not entirely identical.

43. The irresistible force seemed to be met by the immovable object, as the Vice-President put it in argument. To return to **Parliament v Council**, implicit in the Grand Chamber's reasoning in that case is that the Court was adopting a purposive approach: as the purpose of the processing and transfer of data to the United States Government was to further the activities of the state, then the activity of the data processor fell outside the scope of Community law. Applying that principle to this case:

i) the exercise of a legal power by the government of a Member State to require telecommunications operators to transfer data in order to protect national security (i.e. acquisition) is an activity of the State not within the scope of Union law;

ii) on the same basis, the activity of the State in making use of such transferred data for the purpose of protecting national security (i.e. use) must also fall outside Union law;

iii) the activities of commercial undertakings in processing and transferring data for such purposes, as required by national law, (i.e. transfer) must also fall outside the scope of Union law.

Those issues are determined not by analysing whether under the provisions of the DPD and EPD the activity in question constitutes data processing, but whether in substance and effect the purpose of such activity is to advance an "*essential State function*" (Article 4(2) TEU), in this case the protection of national security, through "*a framework established by the public authorities that relates to public security*" (paragraph 56 of **Parliament v Council** set out in paragraph 22(i) above).

44. But for what the Grand Chamber said in **Watson**, it would appear to us that the answer may lie in the conundrum which the Court addressed by preferring Article 15 of the EPD over Article 1(3), though without reference to Article 4 TEU. If in fact it were on the contrary rather to be Article 1(3) which is not to be permitted to be '*deprived of any purpose*', and is to be enforced and applied, as opposed to Article 15, then there can be, and perhaps should be, another approach to Article 15:

i) We have already cited in paragraph 21 above Recital 13 of the DPD, which recites exclusions from the scope of Community Law and of that Directive, where processing "*relates to State security matters".* Recital 11 to the EPD, also there set out, in terms excludes from that Directive activities relating to (inter alia) public and State security matters referred to in Article 15, so that "*the Directive does not affect the ability of Member States to carry out*" interception, or (a fortiori) other less intrusive measures, such as the obtaining and processing of BCD. The proviso is that "*such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the* [ECHR]". This proviso would be satisfied by our conclusions (subject to the reserved issues) in our October Judgment.

ii) Article 1(3) of the EPD, also there set out, states plainly that the Directive does <u>not</u> apply to activities (inter alia) concerning public security and State security, which fall outside the scope of the Treaty. There is no proviso.

iii) Article 15 refers to the legislative measures which may be adopted by Member States to safeguard (inter alia) national security. Until its last sentence it appears to add nothing to Recital 11 (and indeed Recital 13 of the DPD) and to Article 1(3). The last sentence then provides that "*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*". It is this sentence which led the Grand Chamber to the conclusion that the measures in Article 15 fell within the scope of the Directive, and, on its conclusions, the Charter. It seems to us possible,

particularly in the light of the impact of Articles 4 and 5 TEU, and the need to construe the Directive so as to comply with the Treaty, that that sentence may not have such meaning; and certainly did not do so when the Directive was originally adopted, because at that time Article 6(1) and 6(2) TEU were in a different form from that in which they now stand as set out in paragraph 21 above. At that time they read as follows:

> "*1. The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States.*
>
> *2. The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law."*

It seems to us that it may be that the last sentence of Article 15 should thus be construed as nothing more than a reiteration of Recital 11 (with which it is otherwise in conflict) and that the ECHR does, and the Charter does not, apply to those activities excluded under Articles 4 and 5 TEU.

45. This analysis may resolve the otherwise apparent conflict between the construction by the Grand Chamber of Article 15, and the existence of Article 4(2) of the TEU and Recital 11 and Article 1(3) of the EPD, which appear to amount to a positive reservation of sovereignty by the Member States in relation to activities relating to national security. This issue underlies our reasons for making the reference to the Grand Chamber, to which we return below.

<u>The Watson Requirements</u>

46. If the BCD regime is entirely outside the Treaty and the scope of the Directives, as was the case in **Parliament v Council**, then the Watson Requirements would not apply. It is only if the Respondents' arguments as to scope set out above fail that consideration of them will be necessary, and to the extent that they could be applicable to BCD acquired for the purpose of national security.

47. The Watson Requirements are seemingly four:

i) Subject to clarification of the impact of paragraph 119 of the Judgment, to which we shall refer, there is a restriction on any non-targeted access to Bulk Data.

ii) There must be prior authorisation (save in cases of validly established urgency) before any access to data (paragraph 120).

iii) There must be provision for subsequent notification of those affected (paragraph 121).

iv) All data must be retained within the European Union (paragraph 122 and 125: there is doubt as to the effect of paragraph 123, as discussed below).

48. On any basis, it is difficult to see how the ambit of the EPD applies after acquisition by the SIAs, but even if it were widely interpreted, then the first three Watson Requirements might be apt, but the fourth, relating to the later use of the acquired data by a Member State's SIAs would appear to be a further extension.

49. In its simplest form, the dispute between the Respondent and the Claimant can be summarised as follows. The Respondents submit:

a. The BCD regime is not within the scope of the Treaty and the Directive and is only subject to the ECHR.

b. In any event the Watson Requirements cannot and should not apply, because there is no analogy between the activities and the legal basis for such activities under consideration in **Watson** and the BCD regime, as summarised in paragraph 29 above.

The Claimant submits that the Watson Requirements apply, and should be imposed either directly or by analogy, and, although Mr de la Mare accepts that it may be that they derive from a '*partial understanding*' by the Court in **Watson** of the necessities of national security and the operation of the SIAs, the Requirements, if reconsidered, should be reapplied in whole or in part.

50. The Respondents refer to the evidence which we have summarised and accepted in paragraphs 11 to 16 above, and they make a number of powerful submissions:

a. The use of bulk acquisition and automated processing produces less intrusion than other means of obtaining information.

b. The balance between privacy and the protection of public safety is not and should not be equal. Privacy is important and abuse must be avoided by proper safeguards, but protection of the public is preeminent.

c. The existence of intrusion as a result of electronic searching must not be overstated, and indeed must be understood to be minimal.

d. There is no evidence of inhibition upon, or discouragement of, the lawful use of telephonic communication. Indeed the reverse is the case.

e. Requirements or safeguards are necessary but must not, as the Respondents put it, eviscerate or cripple public protection, particularly at a time of high threat.

51. Notwithstanding that communication of personal data to a public authority constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, all these submissions appear to us to have considerable force.

52. The Respondents further submit that the Watson Requirements (or any other safeguards considered by the Grand Chamber to be appropriate over and above any consideration of the ECHR) should not be treated as legal requirements. The Claimant accepts that questions of proportionality are matters for the national court and not the European Court, which will instead set out principles by reference to which proportionality will be assessed; but the Respondents submit that what is being created by reference to the Grand Chamber's judgments in **DRI** and now in **Watson**, if applicable, is that legal requirements are being laid down with which the Member States must comply in order for their conduct to be *in accordance with law*. Mr Eadie submits that the margin of appreciation should be applicable, as in all questions of proportionality, and that, as he puts it, the greatest possible breadth of

discretion is to be afforded to Member States in designing the systems which should apply in a particular context for the collection, retention and accessing of data, and where to strike the balance.

53. We turn to deal with each of the Watson Requirements.

(1) Bulk acquisition and automated processing

54. It is clear that the Grand Chamber in **Watson** did not have the material to address any of the benefits of bulk acquisition in the context of national security in its Judgment, not least because no evidence in that regard was put before them, and in any event, as discussed above, the concentration was on criminal investigation. The evidence is referred to above, and the informed comments of the ISC and of the Anderson Report, which the Claimant did not dispute. As set out above, the Grand Chamber in **Watson** only addressed targeted access. There is in the last sentence of paragraph 119 of the Judgment the only place (other than a brief reference in paragraph 111) where national security is specifically addressed:

> "*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 data might, in a specific case, make any effective contribution to combating such activities.*"

55. However:

a. The references to '*particular situations*' and '*in a specific case*' do not fit the circumstances before us, where the evidence, and in particular the Anderson Report, establishes the necessity of the availability of

bulk, i.e. unspecific, automated processing in the interests of national security.

b. The reference to '*objective evidence*' from which it could be deduced that '*the data of other persons*', might '*in a specific case*' be of use is also inadequate, and appears to refer back to what the Court said in paragraph 111 (quoted above) with regard to the use of *geographic criteria*, which could not practicably be applied in relation to international terrorism.

56. Derived from **Parliament v Council**, Mengozzi AG gives a clearly different picture in his Opinion referred to in paragraph 36(i) above:

> "*205. . . . I do not believe that there are any real obstacles to recognising that the interference constituted by the agreement envisaged is capable of attaining the objective of public security, in particular the objective of combating terrorism and serious transnational crime, pursued by that agreement. As the United Kingdom Government and the Commission, in particular, have claimed, the transfer of PNR data for analysis and retention provides the Canadian authorities with additional opportunities to identify passengers, hitherto not known and not suspected, who might have connections with other persons and/or passengers involved in a terrorist network or participating in serious transnational criminal activities. As illustrated by the statistics communicated by the United Kingdom Government and the Commission concerning the Canadian authorities' past practice, that data constitutes a valuable tool for criminal investigations, (83) which is also of such a kind as to favour, notably in the light of the police cooperation established by the agreement envisaged, the prevention and detection of a terrorist offence or a serious transnational criminal act within the Union.*
>
> . . .
>
> *216. . . ., as the interested parties have explained, the actual interest of PNR schemes, whether they are adopted unilaterally or form the subject matter of an international agreement, is specifically to guarantee the bulk transfer of data that will allow the competent authorities to identify, with the assistance*

of automated processing and scenario tools or predetermined assessment criteria, individuals not known to the law enforcement services who may nonetheless present an 'interest' or a risk to public security and who are therefore liable to be subjected subsequently to more thorough individual checks.

. . .

241. . . . as I have already observed in paragraph 216 of this Opinion, the actual interest of PNR schemes is specifically to guarantee the bulk transfer of data that will allow the competent authorities to identify, with the assistance of automated processing and scenario tools or predetermined assessment criteria, individuals hitherto unknown to the law enforcement services who may nonetheless present an 'interest' or a risk to public security and who are therefore liable to be subjected subsequently to more thorough individual checks. Those checks must also be capable of being carried out over a certain period after the passengers in question have travelled.

242. In addition, unlike the persons whose data was subject to the processing provided for in Directive 2006/24, all those coming under the agreement envisaged voluntarily take a means of international transport to or from a third country, a means of transport which is itself, repeatedly, unfortunately, an vehicle or a victim of terrorism or serious transnational crime, which requires the adoption of measures ensuring a high level of security for all passengers.

243. It is indeed possible to imagine a PNR data transfer and processing scheme that distinguished passengers according to, for example, geographic areas of origin (when they stop over in the Union) or according to passengers' age, minors, for example, prima facie representing a lesser risk for public security. However, in so far as they were considered not to involve prohibited discrimination, such measures, once they became known, might well entail the circumvention of the terms of the agreement envisaged, which would in any event be prejudicial to the effective attainment of one of its objectives.

244. As already indicated, however, it is not sufficient to imagine in the abstract alternative measures that would be less restrictive of individuals' fundamental rights. To my mind, those measures must also present guarantees of effectiveness comparable with those the implementation of which is envisaged with the aim of combating terrorism and serious transnational crime. No other measure which, while limiting the number of persons whose PNR data is automatically processed by the Canadian competent authority, would be capable of attaining with comparable effectiveness the public security aim pursued by the contracting parties has been

brought to the Court's attention in the context of the present proceedings."

57. Our finding set out at paragraph 17 above must be taken into account.

58. The Grand Chamber will need to clarify the meaning and impact of paragraph 119 of its Judgment, and to consider whether the regime of bulk acquisition of BCD in the field of national security is unlawful, if it complies with the ECHR.

(2) Prior authorisation

59. At present the s.94 Directions are made by the Secretary of State, and there is no other prior authorisation. We have considered that the system complies with the ECHR for the detailed reasons set out in the October Judgment (and see in particular paragraph 86). The new Investigatory Powers Act will introduce a system of judicial and other prior authorisations, but, as we have previously concluded, improvement or change in a system does not mean that before such change the system was unlawful (paragraphs 62 and 86 of our October Judgment).

60. The meaning and impact of this Watson Requirement in the different circumstances of BCD is in any event unclear. There are different moments to which this Requirement of prior authorisation might be said to apply:

a. Prior to the making of a s.94 Direction to supply the data – in lieu of or as well as the Secretary of State;

b. Prior to obtaining the data electronically by way of an electronic trawl or search – on each occasion? The protection of national security is

always ongoing and the same data may be accessed on numerous occasions without any genuine intrusion on the private life of any of those whose data is kept there, save for those who may, as a result of the automated processing of data, be of proper intelligence interest to the SIAs;

c. Prior to actual access, whether targeted or resulting from an earlier electronic trawl.

61. We have been satisfied, in particular by reference to the Appendices to our October Judgment that there are sufficient protections from abuse. The Respondents' evidence from relevant witnesses, in particular the third witness statement of the GCHQ witness dated 2 March 2017, is that it would critically undermine the ability of the SIAs to tackle the threat to national security. The Claimant, by reference to the evidence of Ms Graham Wood, a solicitor employed by Privacy International, puts that in issue. We are persuaded by the Respondents' evidence; and Mengozzi AG's Opinion gives no support to a view that further pre-authorisation is required:

> "*268. Likewise, it should be observed that the agreement envisaged does not provide that access to the PNR data is to be subject to prior control by an independent authority, such as the Privacy Commissioner of Canada, or by a court whose decision might limit access to or use of the data and which would deal with the matter following a reasoned request from the CBSA.*
>
> *269. However, the appropriate balance that must be struck between the effective pursuit of the fight against terrorism and serious transnational crime and respect for a high level of protection of the personal data of the passengers concerned does not necessarily require that a prior control of access to the PNR data must be envisaged.*

270. In fact, without its even being necessary to ascertain whether such a prior control would in practice be conceivable and sufficiently effective, given in particular the quantity of data to be examined and the resources available to the independent control authorities, I observe that, in the context of respect for Article 8 of the ECHR by the public authorities who have put in place measures for the interception and surveillance of private communications, the ECtHR has accepted that, save in exceptional circumstances relating in particular to the confidentiality of journalists' sources of information or communications between lawyers and their clients, an ex ante control of those measures by an independent body or a judge is not an absolute requirement, provided that extensive post factum judicial oversight of those measures is guaranteed.

271. In that regard, independently of the doubts prompted by the allocation of the CBSA's surveillance and oversight powers between the 'independent public authority' and the 'authority created by administrative means that exercises its functions in an impartial manner and that has a proven record of autonomy', to which I shall return later, (101) it must be pointed out that Article 14(2) of the agreement envisaged provides that Canada is to ensure that any individual who is of the view that their rights have been infringed by a decision or action in relation to their PNR data may seek effective judicial redress in accordance with Canadian law by way, inter alia, of judicial review. There can be no doubt, having regard to the wording of Article 14(1) of the agreement envisaged and the explanations provided by the interested parties, that that remedy is available against any decision relating to access to the PNR data of the persons concerned, irrespective of their nationality, their domicile or their presence in Canada. In the context of the present procedure of preventive examination of the compatibility of the terms of the agreement envisaged with Articles 7 and 8 of the Charter, the guarantee of such a remedy, the effectiveness of which has not been called in question by any of the interested parties, seems to me to satisfy the condition required by those provisions, read in the light of the interpretation of Article 8 of the ECHR by the ECtHR.

272. Consequently, I consider that the fact that the agreement envisaged has failed to provide that access by the authorised officials of the CBSA to the PNR data is subject to prior control by an independent administrative authority or by a court is not incompatible with Articles 7 and 8 and Article 52(1) of the Charter, in so far as — as is the case — the agreement envisaged requires that Canada guarantee that every person concerned will be entitled to an effective post factum judicial

review of the decisions or actions relating to access to his PNR data."

(3) Notification to those affected

62. This requirement is, as Mr de la Mare points out, expressly subject, in paragraph 121 of the Judgment, to the proviso "*as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities*", but this is in our judgment plainly inadequate as a proviso in the circumstances of national security:

a. The context in **Watson** is plainly of a particular criminal investigation, which has come to an end. The need to protect national security is on-going, as, sadly, is the continuing involvement of large numbers of people in the planning and execution of terrorist activities.

b. The danger of notification is not simply related to the circumstances of a particular investigation or a particular person involved in that investigation, but relates also to further operations, including both the methodology of the obtaining or using of the information and the identity of those involved.

63. We have considered this suggested safeguard, not least because it is referred to in **Weber** (2008) 46 EHRR SE5, in a number of our previous decisions and found that it is not required for compliance with the ECHR. Mengozzi AG is plainly of the same view (paragraph 271, cited above). It would in our judgment be very damaging to national security.

64. In any event it would be very difficult to know how a requirement to give notification should be interpreted in respect of the acquisition or use of a bulk

database and how it could practically be implemented. Are all those whose data is contained in the BCD acquired pursuant to a s.94 Direction to be notified, or all those the subject of an electronic search, or all those who feature in data which is the subject of subsequent or targeted access?

(4) Retention of data within the European Union

65. There are uncertainties about this fourth Watson Requirement:

a. It would seem that it amounts to an absolute bar on transfer of data out of the EU, because the foundation of this requirement is to be found in **DRI**, where it was concluded that it should have been a requirement of the data to be retained by reference to the Data Retention Directive, but in particular because of the wording of paragraph 123 of **Watson** "*the national legislation must make provision for the data to be retained within the European Union*" and paragraph 125 the "*requirement that the data concerned should be retained within the European Union*". However, the Claimant submits that it is not an absolute bar, because of the interpolation of paragraph 123 between paragraphs 122 and 125. That paragraph provides for there to be a review by an independent authority of compliance with the level of protection guaranteed by EU Law, and Mr de la Mare submitted that, by virtue of the reference to Article 8(3) of the Charter, this was to be seen as an independent authority supervising the transfer of data out of the European Union, thus making the bar not absolute. It was however common ground during the hearing that there was uncertainty.

b. The Claimant submits that this is only a requirement for the data itself to remain in the European Union and not the product of the data. If that is so, it is less of a restriction, but the reference in paragraph 123 to a potential claim by a person "*seeking the protection of their data*" would not seem to support this.

66. If there is an absolute bar, it would obviously have a serious impact on the sovereignty of the Member States, and upon their Treaty obligations for the sharing of intelligence information, which might be of considerable importance in the event of a threat to the territorial integrity (Article 4(2) TEU) of a Member State. Further, as discussed in paragraph 46 above, whereas it might be applicable in relation to a case concerning retention of data, it is far from clear that it would apply to a case such as this, where the data had already been supplied to the Member State's SIAs, and it then is to be applied to their subsequent conduct in the exercise of their duty to protect national security.

67. This Requirement would appear to be in clear conflict with **Parliament v Council**, as approved in **Ireland v Parliament**, and with the Opinion of Mengozzi AG, relating as it does to the draft agreement between Canada and the European Union on the transfer and processing of passenger name record data. It would also appear to be in conflict with Article 25 of the DPD "*Transfer of Personal Data to Third Countries*", which of course applies to the EPD by virtue of Article 1(2) of the EPD.

68. This whole question of transfer of data to third parties, including friendly foreign agencies, and whether the present arrangements of the SIAs are

satisfactory in order to comply with the ECHR, remains for our further consideration. What is however clear is that it has not, at any rate to date, been any part of the ECHR issues before us, or of the submissions by the Claimant, that there should be an absolute bar upon the transfer of data out of the European Union to an allied State, including a former Member State.

Conclusion on Watson Requirements

69. We have carefully considered the evidence before us, both from the Claimant and the Respondents, and we are persuaded that if the Watson Requirements do apply to measures taken to safeguard national security, in particular the BCD regime, they would frustrate them and put the national security of the United Kingdom, and, it may be, other Member States, at risk. It is to be hoped that, whether by reconsideration, or clarification, of paragraph 119 of the Judgment, or otherwise, the Grand Chamber will take the opportunity to consider whether any further statement than that the safeguarding provisions of the ECHR should apply is required.

Reference

70. By the end of the hearing it was clear that both parties either agreed to or saw the necessity for a reference to the Grand Chamber, and the need for it is, we suggest, obvious from this Judgment, for the reasons which we have already given and summarise below. Neither party in the event contended that the questions we have considered are either *acte clair,* or *acte éclairé* as a result of the **Watson** judgment.

71. The Claimant did submit that the Respondents were not in a position to dispute that at least the question of scope was *éclairé* by virtue (inter alia) of the following propositions:

a. that the UK Parliament had legislated on the basis of there being an obligation on the Member State under Article 15 of the EPD (particularly in relation to the Communications Act 2003 and the Privacy & Electronic Communications (EC Directive) Regulations 2003). This was vigorously debated before us by an exchange of written submissions, in which it seemed to us the Respondents had the better of the argument. But it does not matter, as it is not alleged that there is any kind of estoppel, and there is plainly now a dispute requiring resolution.

b. that **Gallagher**, **Shingara and Radiom** and **ZZ** were cases in which either the national security point was not taken or, in the case of **ZZ**, was taken in the context of the requirement for a gist, and resolved, and this Tribunal is said to be bound by the views of Richards LJ referred to in paragraph 39 above. But again it is not suggested that there is an estoppel, and even if the Tribunal is bound, that does not prevent a reference: see **Elchinov v Natsionalna Zdravnoosiguritelna Kasa** [2011] 1 CMLR 29 at paragraph 27.

c. that although Article 4 TEU was not referred to in the **Watson** judgment, the Respondents did rely on it in one of its two sets of written submissions. As issue estoppel does not arise, this did not seem to us to be of any substance.

72. We have considered a number of cases in relation to the making of a reference, including **CILFIT** [1982] ECR 3415 and **Da Costa** 1963 ECR 31, and the **Court of Justice's Recommendations to National Courts and Tribunals in Relation to the Initiation of Preliminary Ruling Proceedings** 2016/C439/01, and we are satisfied that there are several reasons for which we either must, or in any event may, make a reference to the Grand Chamber in relation to the BCD regime. In our judgment, it is unclear whether, having regard to Article 4 TEU, and Article 1 (3) EPD, and particularly by reference to the matters set out in paragraph 37 above, the activities of the SIAs in relation to the acquisition and use of BCD for the purposes of national security:

(a) are to any extent governed by Union law,

(b) are subject to the requirements of Article 15(1) EPD in accordance with the decision in **Watson**, or, in accordance with Article 4 TEU and Article 1(3) EPD, and following the decisions in **Parliament v Council** and **Ireland v Parliament**, should be treated as outside the scope of the EPD, or

(c) are subject to the requirements stipulated by the decision in **Watson** at paragraphs 119 – 125 and, if so, to what extent, taking into account the essential necessity of the SIAs to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements.

73. The facts we have found, additionally to those referred to in paragraph 2 above in the October judgment, appear in paragraphs 17, 61 and 69 above.

Expedition

74. We have carefully considered whether we should request expedition of the reference pursuant to Article 105 of the Rules of Procedure. An application to this effect was made to us by the Claimant and opposed by the Respondent.

75. The grounds upon which the Claimant relied in support of its application for expedition were as follows:

a. The issues are important and urgent, and straightforward for the Grand Chamber to decide.

b. In **Watson** there was an order for expedition.

c. If there were an expedited hearing it would remove the necessity for any application to be made to this Tribunal for interim relief.

76. The Respondents' responses, which we accept, were as follows:

a. The issues are not at all straightforward, and their importance to the Member States would run counter to any foreshortening of the opportunity for other Member States to consider whether to take any part, and to participate if so advised.

b. In **Watson** there were three grounds for the order of expedition, only the third of which was its importance, as appears from the order of the

President of the Court in that case dated 1 February 2016, the other two plainly being primary and significant:

i. The desirability of joining **Watson** with the Swedish case, which was already far advanced.

ii. The existence of the 'sunset clause' expiring 31 December 2016 in relation to DRIPA referred to in paragraph 20 above. In the event, the Grand Chamber's Judgment of 21 December 2016 only just met that deadline.

Those reasons plainly do not apply in this case.

c. That if the Claimant wishes to make an application for interim relief they are free to do so.

77. In the circumstances, for the reasons set out in paragraph 76 above, we do not consider it appropriate to make any request for expedition.

POSTSCRIPT

78. Since the completion of this Judgment by the Tribunal, the Grand Chamber has delivered its Opinion 1/15 (ECL1:EU:C: 2017:592) dated 26 July 2017 (in relation to which the Tribunal recited some paragraphs of the Opinion of Mengozzi AG of 8 September 2016 in paragraphs 36(i), 56, 61 and 63 above). We have not therefore taken into account the Grand Chamber's Opinion in reaching our determinations in this Judgment. We invited brief submissions from the parties as to the effect of that Opinion on our Judgment. The Claimant submits that this Opinion supports its interpretation of **Watson** and

extends it to cover issues arising in the context of national security. The Respondents point out that the Grand Chamber's Opinion did not address or consider Article 4 of the Treaty or Article 1(3) of the EPD or the Grand Chamber decisions referred to in paragraph 72 above, or the question of the scope of Union law addressed in paragraphs 29 to 45 above, and, so far as concerns the issue of the Watson Requirements, that it allows (at paragraph 186-189) for automated processing and did not disapprove certain of the paragraphs of the Opinion of Mengozzi AG above. Both parties are however agreed that the delivery of the 26 July Decision by the Grand Chamber reinforces the need for the Reference which we are making and it is therefore not necessary for this Tribunal to express any views on the effect of the Opinion on the answers to the issues which are to be referred.