IN THE INVESTIGATORY POWERS TRIBUNAL **CASE NO. IPT/15/110/CH**
BEFORE THE PRESIDENT,
SIR RICHARD MCLAUGHLIN, MR CHARLES FLINT QC
AND MS SUSAN O'BRIEN QC

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

- and -

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS
(4) SECURITY SERVICE
(5) SECRET INTELLIGENCE SERVICE

Respondents

ORDER FOR REFERENCE
TO THE COURT OF JUSTICE OF THE EUROPEAN UNION

UPON the Tribunal's judgment of 8 September 2017

AND UPON hearing counsel for the Claimant and the Respondents

IT IS ORDERED THAT:

1. The questions set out in the Annex to this Order shall be referred to the Court of Justice of the European Union ('**Court of Justice**') for a preliminary ruling pursuant to Article 267 of the Treaty on the Functioning of the European Union. The Annex to this Order and accompanying documents shall be sent to the Court of Justice forthwith.

2. With the exception of the matters to be determined at the hearing listed for 17–19 October 2017, any further proceedings in this case shall be stayed until the Court of Justice has given its preliminary ruling on the questions set out in the Annex hereto, or until further order of the Tribunal.

THE PARTIES TO THE CASE ARE:

Claimant: PRIVACY INTERNATIONAL

Contact: Mark Scott, Bhatt Murphy Solicitors, 10 Tyssen Street, Dalston, London E8 2FE. Telephone: +44 20 7729 1115 Fax: +44 20 7729 1117. Email M.Scott@bhattmurphy.co.uk

Respondents SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS, SECRETARY OF STATE FOR THE HOME DEPARTMENT, GOVERNMENT COMMUNICATIONS HEADQUARTERS, SECURITY SERVICE SECRET INTELLIGENCE SERVICE,

Contact: Ellie Oakley, Government Legal Department, One Kemble Street, London, WC2B 4TS. Telephone: +44 207 210 8505 Fax +44 207 210 3152 Email: Ellie.Oakley@TSOL.GSI.GOV.UK

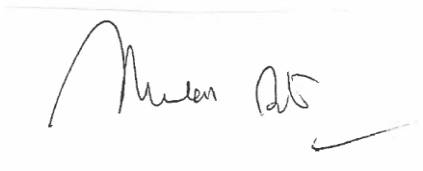
REFERRING COURT

President: The Hon Sir Michael Burton
Address: Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZG

Tel: +44 207 035 3711
Email: InvestigatoryPowersTribunal@ipt.gsi.gov.uk

Contact: Tribunal Secretary
Susan Cobb

SIGNED



The Hon Sir Michael Burton
President
Investigatory Powers Tribunal

18 October 2017

ANNEX

IN THE INVESTIGATORY POWERS TRIBUNAL **CASE NO. IPT/15/110/CH**

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

REQUEST FOR A PRELIMINARY RULING
PURSUANT TO ARTICLE 267 TFEU

INTRODUCTION & SUMMARY

1. This case relates to national legislation governing the acquisition and use by the Security & Intelligence Agencies ('SIAs') of the United Kingdom of Bulk Communications Data ('BCD'). It concerns the balance between the State's ability, through the SIAs, to protect its population against terror and threats to life, and the protection of privacy of the individual.

2. The claimant is Privacy International, a non-governmental human rights organisation, working in the field of defending human rights at both national and international levels. The Respondents are the Secretary of State for Foreign and Commonwealth Affairs, the Secretary of State for the Home Department, and the three United Kingdom SIAs, i.e. Government Communications Headquarters (GCHQ), the Security Service (MI5), and the Secret Intelligence Service (MI6).

3. Subject to certain reserved issues that remain under consideration, this Tribunal has determined that the current national legislative regime under consideration ('the BCD regime') has, but only since 2015, satisfied the requirements of the European Convention on Human Rights and Fundamental Freedoms ('ECHR'). This request for a

preliminary ruling concerns whether the BCD regime is within the scope of EU Law and, if so, whether, and how, any requirements of EU law that go beyond those applicable under the ECHR apply to the BCD regime.

4. The request for a preliminary ruling asks the Court of Justice to clarify the basis on which EU law may apply to the national security activities of the SIAs of a Member State, having regard to Article 4 TEU, which provides that the European Union shall respect the essential state function of safeguarding national security, so that national security remains the sole responsibility of each Member State.

5. The context and the reasons for this request are set out more fully in this Tribunal's judgment of 8 September 2017, a copy of which is annexed to this request.[1]

RELEVANT FACTUAL CONTEXT - BCD

6. Pursuant to section 94 of the Telecommunications Act 1984 ('the 1984 Act') the Secretary of State may, after consultation with an operator of a Public Electronic Communications Network (**'PECN'**), give to that operator such general or specific directions as appear to the Secretary of State to be necessary in the interests of national security or relations with a foreign government. Also, if it appears to the Secretary of State to be necessary in the interests of national security or relations with a foreign government, the Secretary of State may give to that PECN operator a direction requiring the operator to do, or not to do, a particular thing specified in the direction.

7. The SIAs acquire BCD pursuant to directions made by the Secretary of State under section 94 of the 1984 Act, and have done so since 2001 (in the case of GCHQ) and 2005 in the case of the Security Service (MI5). Copies of redacted versions of the two original forms of direction are attached hereto as Annex 1. The BCD provided by PECNs under such directions includes 'Traffic Data' and 'Service Use Information', as defined in national legislation. This may include the 'who, where, when and how' of a communication. It does not contain the content of communications. Section 94

[1] Ref. IPT/15/110/CH, the Judgment is also available at: www.ipt-uk.com/docs/Privacy%20International%20v%20SSFCA%20and%20Ors%20September%202017.pdf and at www.bailii.org/uk/cases/UKIPTrib/2017/IPT_15_110_CH.html

directions have not been, and cannot be, used to authorise the interception of the content of communications; interception of content is governed by other national legislation.

8. The BCD acquired from PECNs is held securely by the SIAs to assist in the work of the SIAs. A fundamental feature of many of the SIAs' techniques of interrogating BCD is that the techniques are non-targeted, i.e. not directed at specific, known targets. A 2015 report by the Intelligence & Security Committee of the United Kingdom Parliament observed that: "*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.*"[2]

The Anderson Report

9. An independent report published on 19 August 2016 by David Anderson QC, the then United Kingdom Independent Reviewer of Terrorism Legislation (the 'Anderson Report'), evaluated the operational case for the use of, *inter alia*, BCD. The Anderson Report is important because it is based on a review conducted by a team of independent persons, 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.

10. The Anderson Report concluded, *inter alia*, that:

    i. there is a proven operational case for the use of the powers to obtain and use BCD;

[2] Intelligence and Security Committee of Parliament, '*Privacy and Security: A modern and transparent legal framework*', 12 March 2015, §77K, available at http://isc.independent.gov.uk/news-archive/12march2015.

ii. those powers are used across the range of activities of the SIAs, from cyber-security, counter-espionage and counter-terrorism to child sexual abuse and organised crime; and

iii. such powers play an important part in identifying, understanding and averting threats to the United Kingdom and elsewhere.

11. Included in the Anderson Report case studies were two case studies which illustrated the necessity for access to BCD 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."*

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

13. The overall conclusion of Mr Anderson QC, at §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 before this Tribunal, which demonstrates that the use of BCD is of critical value to the SIAs, and is of particular value in identifying potential threats by persons who are not presently the target of any investigation. These bulk 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 witnesses in this case 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. 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*". The MI5 witness who gave evidence in these proceedings gave evidence 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."

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. The powers 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 a bulk 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. This Tribunal has considered detailed evidence and arguments on the role of BCD in supporting the work of the SIAs to counter serious threats to public safety, particularly from international terrorism, and in circumstances where those who pose such threats are able to use increasingly sophisticated methods to protect their communications. All of the evidence and materials that this Tribunal has seen are consistent with what is set out in paragraphs 10 to 16 above. We accept that evidence and we agree with it. We have determined that the BCD capabilities of the SIAs, including the capability to

acquire and use BCD, are essential to the protection of the national security of the United Kingdom.

THE DISPUTE IN THE NATIONAL PROCEEDINGS

18. In addition to the matters above, this Tribunal has also considered detailed evidence and arguments relating to the safeguards that apply to the acquisition and use of BCD by the SIAs, including the arrangements for storing and retaining BCD, procedures for accessing BCD and disclosing BCD outside the SIAs, and independent oversight arrangements. Subject to certain reserved issues that remain under consideration, we have determined that the current national legislative regime relating to the acquisition and use of BCD by the SIAs satisfies the requirements of the ECHR.[3]

19. The present stage of these proceedings concerns the impact of the Grand Chamber's judgment in 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* (EU:C:2016:970) ('*Watson*') upon the conclusions we have reached, by reference to the ECHR, as to the appropriate balance 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.

20. The section 94 regime is unlike the provisions of the Data Retention and Investigatory Powers Act 2014 ('DRIPA'), which was the national legislation considered in *Watson*, under which a public telecommunications operator 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 and other public authorities as and when called upon. Unlike DRIPA, section 94 of the 1984 Act requires communications data to be delivered up by the operator to the SIAs, so as to constitute BCD in the custody of the SIAs. Access to the BCD held by the SIAs 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

[3] See this Tribunal's Judgment of 17 October 2016, available at www.ipt-uk.com/docs/Bulk%20Data%20judgement%20-%20June%202017.pdf and at http://www.bailii.org/uk/cases/UKIPTrib/2016/15_110-CH.html

miniscule quantity of the data trawled is ever examined. There is thus no genuine intrusion to any save that miniscule proportion.

21. The Claimant submits that, in the light of *Watson*, the intrusion through such bulk techniques is substantial, and the acquisition (and access to and use of) BCD is unlawful at EU law. The Claimant submits that the requirements applicable to retained communications data, specified by the Grand Chamber in paragraphs 119 to 125 of *Watson* ('the *Watson* Requirements'), apply and should be imposed either directly or by analogy, in this national security context.

22. The Respondents submit that no such conclusion can be reached and 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 from the serious crime purposes at issue in *Watson*;

    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, and with previous decisions of the Grand Chamber, referred to below; and

    iii. the safeguards of ECHR Article 8 are in any event sufficient to control the activities of the Member 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.

APPLICABLE LAW

23. Applicable national legislation:

    - Section 94, Telecommunications Act 1984.

24. Applicable EU Law:

    - TEU, Articles 4, 5, 6
    - TFEU, Article 16
    - EU Charter of Fundamental Rights, Articles 7, 8 and 51

- Directive 95/46/EC ('the Data Protection Directive'), Recital 13, Article 3
- Directive 2002/58/EC ('the e-Privacy Directive'), Recital 11, Articles 1 and 15
- Joined cases C-317/04 & C-318/04 *Parliament v. Council* (EU:C:2006:346), §§56-59
- Joined cases C‑293/12 & C‑594/12 *Digital Rights Ireland* (EU:C:2014:238)
- Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB* (EU:C:2016:970)

PROVISIONAL CONCLUSIONS ON EU LAW

25. The first of the two joined cases in *Watson* related to Swedish laws 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. The legislation at issue in *Watson*, DRIPA, 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 section 22(2) of the Regulation of Investigatory Powers Act 2000. It is clear that (save for a 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*.

26. By contrast, as described above, section 94 of the 1984 Act relates to directions by the Secretary of State to PECNs to supply BCD to the SIAs (i.e. not requiring the PECN operators to retain data themselves), as necessary and proportionate in the interests of national security or relations with foreign governments.

27. The Respondents argue that *Watson* was addressing the targeted access of data in criminal investigations and not the needs of national security, and that *Watson* does not consider Article 4(2) of the TEU and the consequence of the exclusion of (in particular) national security from the ambit of the Treaties. They maintain that, since the Member States retain sole responsibility for national security, and have not conferred the essential State functions of national security on the Union, 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.

28. The Respondents rely, in particular, on joined cases C-317/04 & C-318/04 *Parliament v. Council* (EU:C:2006:346), in which, at §§56-59, the Grand Chamber held that the transfer of passenger name record data by airline operators to the U.S. Bureau of Customs and Border Protection was processing of personal data falling within a framework relating to public security, outside the scope of Community law, as referred to in Article 3(2) of the Data Protection Directive (Directive 95/46/EC). The Grand Chamber found that the data processing in question was processing required not for the supply of services, but for public security purposes.[4]

29. The exclusion of certain activities from the jurisdiction of the Union is clearly explained in Case C-51/15 *Remondis* (EU:C:2016:985), in relation to an activity excluded by Article 4(2) TEU, namely the organisation of local government.[5] The Respondents have also referred to the European Council Notice 2016/C691/01 of February 2016, which records the European Council's view that: "*Article 4(2) of the Treaty on European Union confirms that national security remains the sole responsibility of each Member State. This does not constitute a derogation from Union law and should therefore not be interpreted restrictively. In exercising their powers, the Union institutions will fully respect the national security responsibility of the Member States.*"

30. The Claimant maintains that national security does not constitute an ouster of jurisdiction, or a framework outside the Treaty, but a derogation. The Claimant submits that once you choose to have an exception, which is used to derogate from or qualify the rights and obligations in Article 5 of the e-Privacy Directive, that must conform with the minimum standards supplied by EU law. The Claimant also 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, should be read as solely conferring administrative or executive responsibility. We do not find this to be very persuasive, or consistent with the principle of conferral set out in Article 5 TEU.

[4] This is made clear, and was a distinction adopted, by the Grand Chamber in its later judgment in Case C-301/06 *Ireland v Parliament* (EU:C:2009:68), §§88, 91. See also the Opinion of Advocate General Mengozzi of 8 September 2016 in *Opinion 1/15* (EU:C:2016:656), §85

[5] See the Opinion of Advocate General Mengozzi of 30 June 2016, §§38, 41-42 and the Judgment of the Court at §§41-42.

31. The Claimant submits in any event that the activities of the security services of Member States are outside the scope of the Treaties 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. The Claimant points to the treatment of national security derogations in the context of free movement, referring e.g. to case C-387/05 *Commission v Italian Republic*, §45, and Case C-300/11 *ZZ (France)*, §38.

32. The Claimant therefore submits that *Watson* is binding and should be applied directly in the national security context, even though the facts are not entirely identical.

33. This Tribunal considers that the judgment in *Parliament v Council* is of direct significance to the present case. Notwithstanding that the processing and transfer of data addressed in that case was effected by commercial undertakings, whose activities were subject to the Data Protection Directive, 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) of that Directive.

34. The judgment in *Parliament v. Council* appears to be on all fours with this case and to point to the opposite conclusion than that reached by the Grand Chamber in *Watson*. Like this case, *Parliament v. Council* was concerned with the transfer of personal data by commercial operators to State authorities pursuant to a framework concerned with protecting the interests of national security. Implicit in the Grand Chamber's reasoning in *Parliament v. Council* 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.

35. Applying that principle to this case, it appears to this Tribunal that:

    i. the exercise of a legal power by the government of a Member State to require telecommunications operators to transfer data to the State 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.

36. Those issues are determined not by analysing whether, under the provisions of the Data Protection Directive and e-Privacy Directive, 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*).

37. But for what the Grand Chamber said in *Watson*, it would appear to this Tribunal that the answer may lie in the conundrum which the Court addressed by preferring Article 15 of the e-Privacy Directive 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[6], then there can be, and perhaps should be, another approach to Article 15:

i. Recital 13 of the Data Protection Directive recites exclusions from the scope of Community Law and of that Directive, where processing "relates to State security matters". Recital 11 to the e-Privacy Directive 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*

[6] Contrast paragraph 73 of the Grand Chamber's Judgment in *Watson.*

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 2016 Judgment, which finds the BCD regime to be compatible with the ECHR.

ii. Article 1(3) of the e-Privacy Directive states plainly that the Directive does not 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 of the e-Privacy Directive 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 Data Protection Directive) 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 Treaties, 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.

38. It seems to this Tribunal that it may be that the last sentence of Article 15 of the e-Privacy Directive 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 EU law and the Charter does not, apply to those activities excluded under Articles 4 and 5 TEU.

39. 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 e-Privacy Directive, which appear to amount to a positive reservation of sovereignty by the Member States in relation to activities relating to national security.

FINDINGS ON THE APPLICATION OF THE WATSON REQUIREMENTS

40. If our conclusion on the application of EU law to national security activity is wrong, the question arises as to the practical application of the *Watson* Requirements to the BCD regime. The *Watson* Requirements, derived from §§119-125 of the Grand Chambers' judgment, are seemingly four:

    i. subject to clarification of the impact of §119 of the Judgment, to which we refer below, there is a restriction on any non-targeted access to BCD;

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

    iii. there must be provision for subsequent notification of those affected (§121); and

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

41. On any basis, it is difficult to see how the ambit of the e-Privacy Directive applies after acquisition of BCD 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.

(1) BCD and automated processing

42. It is clear that the Grand Chamber in *Watson* did not have the material to address any of the benefits of BCD in the context of national security in its judgment, not least because no evidence in that regard was put before the Court, and in any event, as discussed above, the focus was on criminal investigation. The evidence is referred to above, including the informed comments of the Intelligence & Security Committee of the United Kingdom Parliament and of the Anderson Report. The Claimant in the present case does not dispute this evidence.

43. The judgment in *Watson* addressed only targeted access. There is, however, in the last sentence of §119 of the Judgment the only place (other than a brief reference in §111) where national security is specifically addressed. In §119 of *Watson* the Grand Chamber refers to "*particular situations, where for example vital national security, defence or*

public security interests are threatened by terrorist activities" and where *"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.*"

44. 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; and

    (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 §111 with regard to the use of geographic criteria, which could not practicably be applied in relation to international terrorism.[7]

45. We refer again to our factual finding at paragraph 17 above and ask the Grand Chamber to clarify the meaning and impact of §119 of its Judgment, and to consider whether the regime relating to BCD in the field of national security is unlawful, in circumstances where, as this Tribunal has determined, it complies with the ECHR.

(2) Prior authorisation

46. At present the section 94 directions are made by the Secretary of State, and there is no other form of prior authorisation. Subject to the reserved issues, we have concluded that the system complies with the ECHR for the detailed reasons set out in our judgment of 17 October 2016, in particular our view that, provided there are otherwise adequate safeguards, the absence of prior judicial authorisation or of subsequent notification to a

[7] Derived from *Parliament v Council*, Mengozzi AG gives a clearly different picture of EU law's attitude to non-targeted processing by the State in his Opinion of 8 September 2016 in *Opinion 1/15* (EU:C:2016:656), §§205, 216 and 241-244.

subject of interception does not render the system in breach of Article 8 ECHR (though we emphasise that this case does not concern interception of content).

47. 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.

48. We have found that there are sufficient protections from abuse in the national regime.[8] The evidence which we have considered shows that a requirement for further authorisation prior to either an electronic trawl or actual access to specific data or both would critically undermine the ability of the SIA's to tackle some threats to national security.[9]

(3) Notification to those affected

49. This requirement is expressly subject, in §121 of the *Watson* Judgment, to the proviso "*as soon as that notification is no longer liable to jeopardize the investigations being*

[8] In particular for the reasons set out in the Appendices to our October 2016 Judgment.
[9] We also note that Advocate General Mengozzi's Opinion in *Opinion 1/15* at §§268-272 gives no support to a view that further pre-authorisation is required.

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 ongoing, 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.

50. We have considered this suggested safeguard, not least because it is referred to in *Weber & Saravia v. Germany*[10] and in a number of our previous decisions, and have found that it is not required for compliance with the ECHR, in particular because there are suitable alternative mechanisms, such as the operation of this Tribunal, which the European Court of Human Rights has found to be effective as a means of protecting rights under Article 8 ECHR.[11] It would in our judgment be very damaging to national security to impose such a requirement.

51. 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 BCD 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

52. There are also uncertainties about this fourth *Watson* Requirement:

(a) It might arguably be read as amounting to an absolute bar on transfer of data out of the EU, because the foundation of this requirement is to be found in *Digital*

[10] Application No. 54934/00, Admissibility Decision of 29 June 2006.
[11] Advocate General Mengozzi was plainly of the same view in *Opinion 1/15*

Rights Ireland (EU:C:2014:238), 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 §123 of *Watson* "*the national legislation must make provision for the data to be retained within the European Union*" and §125 the "*requirement that the data concerned should be retained within the European Union*". However, the Claimant in the present case submits that it should not be read as an absolute bar, because of the interpolation of §123 between §§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 the Claimant 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. However, there is 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 §123 to a potential claim by a person "*seeking the protection of their data*" would not seem to support this.

53. If there were to be an absolute bar on transfer of BCD outside the EU, 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.

54. Such a requirement would appear to be in clear conflict with *Parliament v Council*, as approved in *Ireland v Parliament*, and with the Opinion of Advocate General Mengozzi in *Opinion 1/15*, relating as it does to the draft agreement between Canada and the European Union on the transfer and processing of passenger name record data.[12] It would also appear to be in conflict with Article 25 of the Data Protection Directive, '*Transfer of Personal Data to Third Countries*', which applies to the e-Privacy Directive by virtue of Article 1(2) of the e-Privacy Directive.

[12] The Tribunal did not take into account the decision of the Grand Chamber in this case as it was delivered after the finalisation of its Judgment

55. This 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. It has not, 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.

Conclusion on the application of the Watson Requirements

56. We have carefully considered the evidence before us and we have concluded that if the *Watson* Requirements do apply to measures taken to safeguard national security, in particular the BCD regime, they would frustrate those measures and put the national security of the United Kingdom at risk.

57. We hope that, whether by reconsideration, or clarification, of §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.

58. In our judgment, it is unclear whether, having regard to Article 4 TEU, and Article 1(3) e-Privacy Directive, 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(3) e-Privacy Directive in accordance with the decision in Watson, or, in accordance with Article 4 TEU and Article 1(3) e-Privacy Directive, and following the decisions in *Parliament v Council* and *Ireland v Parliament*, should be treated as outside the scope of the e-Privacy Directive, or

    (c) are subject to the requirements stipulated in *Watson* at §§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.

FINDINGS OF FACT

59. The relevant findings of fact as determined by this Tribunal are as follows:

i. the SIAs' capabilities to use BCD supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation. We accept and agree with the evidence described in paragraphs 10 to 16 above;

ii. in particular, a fundamental feature of the SIAs' use of BCD is to discover previously unknown threats to national security by means of non-targeted bulk techniques which are reliant upon the aggregation of the BCD in one place. Its principal utility lies in swift target identification and development, as well as providing a basis for action in the face of imminent threat;

iii. the provider of an electronic communications network does not retain the BCD (beyond the period of their ordinary business requirements). The BCD is retained by the State (the SIAs) alone;

iv. the use of BCD and automated processing produces less intrusion than other means of obtaining information, and the degree of intrusion as a result of electronic searching of BCD should not be overstated;

v. the safeguards surrounding the use of BCD by the SIAs are now, subject to the reserved issues, consistent with the requirements of the ECHR, and are sufficient to prevent abuse;

vi. the imposition of the *Watson Requirements* if applicable, would critically undermine the ability of the SIAs to safeguard national security, and thereby put the national security of the United Kingdom at risk.

QUESTIONS REFERRED

In circumstances where:

a. the SIAs' capabilities to use BCD supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation;

b. a fundamental feature of the SIA's use of the BCD is to discover previously unknown threats to national security by means of non-targeted bulk techniques which are reliant upon the aggregation of the BCD in one place. Its principal utility lies in swift target identification and development, as well as providing a basis for action in the face of imminent threat;

c. the provider of an electronic communications network is not thereafter required to retain the BCD (beyond the period of their ordinary business requirements), which is retained by the State (the SIAs) alone;

d. the national court has found (subject to certain reserved issues) that the safeguards surrounding the use of BCD by the SIAs are consistent with the requirements of the ECHR; and

e. the national court has found that the imposition of the requirements specified in §§119-125 of the judgment of the Grand Chamber in 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* (ECLI:EU:C:2016:970) ('*the Watson* Requirements'), if applicable, would frustrate the measures taken to safeguard national security by the SIAs, and thereby put the national security of the United Kingdom at risk;

1. Having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications (the "e-Privacy Directive"), does a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies ('SIAs') of a Member State fall within the scope of Union law and of the e-Privacy Directive?

2. If the answer to Question (1) is 'yes', do any of the *Watson* Requirements, or any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State? And, if so, how and to what extent do those requirements apply, 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?

ACCOMPANYING DOCUMENTS

This request for a preliminary ruling is accompanied by the following documents:

(i) Judgment of the Investigatory Powers Tribunal dated 17 October 2016.

(ii) Judgment of the Investigatory Powers Tribunal dated 8 September 2017.

(iii) Section 94, Telecommunications Act 1984.

(iv) Two sample directions made under section 94, Telecommunications Act 1984.