IN THE COURT OF JUSTICE OF THE EUROPEAN UNION

CASE C-623/17

PRIVACY INTERNATIONAL

-V-

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

WRITTEN OBSERVATIONS OF THE UNITED KINGDOM

The United Kingdom is represented by Simon Brandon of the Government Legal Department, acting as Agent, and by Daniel Beard QC and Robert Palmer, Barristers.

Submitted by
Simon Brandon

Agent for the United Kingdom
Government Legal Department
Room 3/01
1 Horse Guards Road
London
SW1A 2HQ

and
Daniel Beard QC
Robert Palmer
Barristers

Service may also be made by fax or by email:
Fax: 00 44 20 7276 0184
Email: simon.brandon@cabinetoffice.gov.uk

19 February 2018

INTRODUCTION AND BACKGROUND

1. Pursuant to Article 23 of the Protocol on the Statute of the Court of Justice of the European Union, the United Kingdom submits the following written observations in relation to the questions referred for a preliminary ruling under Article 267 TFEU by the Investigatory Powers Tribunal ("**the Tribunal**") in its order for reference registered on 6 November 2017 ("**the Order for Reference**" or "**OfR**").

2. This case is concerned with Member States' legal framework and activities for the protection of the State's national security. The activities in question are core and critical aspects of that protection. The context, and the relevant factual basis on which the Reference proceeds, are set out in clear terms in the Order for Reference.

3. The referring Tribunal is an independent and expert tribunal established under sections 65-69 of the Regulation of Investigatory Powers Act 2000 ("**RIPA**")[1]. It has a very extensive jurisdiction to consider and adjudicate on complaints against the Security and Intelligence Agencies ("**the Agencies**" or "**SIAs"**). It is believed that the Tribunal was the first court of its kind to establish *'inter partes'* hearings in open court in the security field**.**

   (1) It is able to hold hearings in public, including full adversarial argument, as to whether the conduct alleged, if it had occurred, would have been lawful.

   (2) It may then hold *'closed'* hearings in private to apply the legal conclusions from the open hearings to the facts, based on a consideration of classified intelligence material. As it did in this case, the Tribunal also has the power to instruct Counsel to the Tribunal – as an '*amicus curiae*' – to advise the Tribunal. Counsel to the Tribunal has full access to all the confidential and secret files produced to the Tribunal, and is able to advance arguments in any '*closed'* hearing to support a claimant's case with full knowledge of that evidence.[2] The Agencies are required (by section 68(6) RIPA) to provide any information the Tribunal requests. The Tribunal can also demand clarification or explanation of the information provided. The Tribunal receives full and frank disclosure of relevant, often highly sensitive,

[1] The role of the Tribunal was considered in detail by the European Court of Human Rights in *Kennedy v United Kingdom* [2011] EHRR 4. The Court held that the Tribunal's operation was consistent with Article 6 ECHR, and offered an effective remedy consistently with Article 13 ECHR in response to an alleged violation of rights arising from alleged interception of communications.

[2] See the Investigatory Powers Tribunal's website: http://www.ipt-uk.com, in particular at http://www.ipt-uk.com/content.asp?id=10, http://www.ipt-uk.com/content.asp?id=13 and http://www.ipt-uk.com/content.asp?id=20.

material from those bodies from whom it requests information. In the present case, it received extensive witness statements from each of the Agencies, which annexed substantial amounts of classified material for the Tribunal's review.

4. It is against that background that the Tribunal made its findings of fact in the present case. Its conclusions were based on specific and detailed evidence before it (OfR, §17) and included evidence about particular, specific examples of the importance of that capability (see eg OfR at §11).[3] Its findings of fact are summarised at OfR, §59. Its two central findings of fact were, **first**, that the Agencies' power to obtain and access BCD from an electronic communications network provider is essential to the protection of the national security of the United Kingdom (OfR, §59(i)-(ii)); and, **secondly**, that the application of the *Watson* requirements would critically undermine the ability of the Agencies to safeguard national security, and thereby put the national security of the United Kingdom at risk (OfR, §59(vi)).

5. The conclusions of the Tribunal are echoed by the assessment of the United Kingdom Independent Reviewer of Terrorism Legislation (an office recently held by David Anderson QC), who was tasked with reviewing the case for the Agencies' power to acquire and use bulk data. He was able to obtain and review classified material, and question intelligence officers on the use and justification for their powers (see OfR, §§9-13). Furthermore, the Intelligence and Security Committee of Parliament has also considered the importance of the use of bulk data. That Committee is established by Parliament under statute and made up of distinguished Parliamentarians who have further responsibility for the oversight of the Agencies and other parts of the UK intelligence community. Their duties include overseeing the agencies' activities, policies, expenditure, administration and operations. Their conclusions on the importance of the use of bulk data are to substantially the same effect as those of the Tribunal and are referred to at OfR §8.

6. Threats to a State's national security represent a direct challenge to its ability to perform its essential state function of the protection of its people, its territorial integrity and its sovereignty. Such threats are varied and unpredictable in their nature, their extent and their source. Threats can emanate from hostile States, organised groups of insurrectionists and terrorists, or physically unconnected individuals inspired by a

[3] The Tribunal expressly accepted and agreed with the evidence described in §§10 to 16 OfR: see §§17 and 59(i)-(ii) OfR

shared ideology of violence. Threats can emerge unannounced and change at speed. Illustrative (but non-exhaustive) examples may be terrorism and sabotage, actions intended to overthrow or undermine parliamentary democracy, cyber attacks affecting public services, border incursions, espionage, or the development by stealth of nuclear, biological or chemical weapon capability or intention. The nature and level of threats, and therefore the nature of an appropriate measure to illuminate and respond to such threats, may also vary considerably between States. The way in which Member States seek to pre-empt these threats and stay ahead of them will vary and touches on some of the most essential and sovereign aspects of a state's responsibility.

7. Responsibility for protecting the United Kingdom's national security lies particularly with the Agencies. That responsibility is a heavy and difficult one – as the repeated and appalling recent attacks in the United Kingdom and elsewhere across Europe indicate only too clearly. The United Kingdom faces an acute threat.[4]

8. Under directions made under section 94 of the Telecommunications Act 1984 ("**section 94 directions**"), an operator of a Public Electronic Communications Network ("**Public network**" or "**PECN**") may be required to provide bulk communications data ("**BCD**") to the Agencies. That power is exercisable only where this is necessary and proportionate in the interests of national security. That provision is the essential first step in the critical ability of the Agencies to hold the BCD securely and interrogate it in the fulfilment of their protective functions – particularly with a view to threat identification.

9. One particular feature is to be noted at the outset in relation to the necessity of the Agencies' ability to use bulk data in this way. It is a core part of the Agencies' functions to seek, as effectively as possible, to identify threats before an attack is made. The Tribunal found that a fundamental feature of the Agencies' 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 threat identification and development, as well as providing a basis for action in the face of imminent threat. Having considered extensive evidence, the Tribunal recognised the importance of the bulk data both in developing fragmentary

[4] For example, Europol publishes statistics of the number of failed, foiled or completed terrorist attacks in the EU. In 2016 there were 142 of these recorded, with more than half (76) recorded in the UK. See https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2018/01/Terrorism-Acts-in-2016.pdf at paragraph 2.4.

intelligence to identify targets and in doing so with sufficient speed to prevent atrocities. See e.g. OfR, §§8, 13, 14.

10. Against this background the United Kingdom makes two broad submissions:

    (1) First, that competence for Member States' national security lies exclusively with the Member States. It is not a competence which has been conferred by the Treaties on the EU. To the contrary, Article 4(2) TEU clearly and expressly identifies national security as being the **sole** responsibility of Member States. The Tribunal's first question should accordingly be answered in the negative.

    (2) Alternatively secondly, that there is no proper basis for seeking to impose the sorts of requirements discussed in *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson and Others*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970 (***"Watson"***) in the present context. The Judgment in *Watson* did not consider the requirements that should apply in a national security context such as the present. The requirements there discussed are unsuited to the context of national security. As the Tribunal found in clear and stark terms, their imposition in the present context would critically undermine the ability of the State to protect national security and thus its citizens. Furthermore, the present case has been referred on the basis of a specific finding by the Tribunal – after detailed consideration – that the relevant domestic legal regime is fully compliant with the European Convention on Human Rights ("**ECHR**"). The Tribunal found that that regime had sufficient and extensive legal safeguards built into it and privacy rights were properly protected. Accordingly, if the Tribunal's second question arises, it is to be answered in the negative.

THE UNITED KINGDOM'S RESPONSE TO THE QUESTIONS REFERRED

QUESTION 1

11. The answer to the first question is that a direction by a Secretary of State to a provider of a Public Network that it is necessary and proportionate for it to provide bulk communications data to the Agencies of a Member State in the interests of national security does not fall within the scope of Union law or of the e-Privacy Directive.

I. The meaning and effect of Article 4(2) TEU

12. The factual basis on which this issue arises is that the acquisition of data, such as BCD, by the Agencies for analysis for national security purposes is a paradigm example of national security activity, core to the Agencies' ability to function. Agencies rely on the acquisition of data to provide the raw material of intelligence. As the Tribunal found, the Agencies' capabilities to acquire and use BCD supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counterterrorism, counter-espionage and counter-nuclear proliferation (OfR, §59(i)).

Articles 4 and 5 TEU

13. Article 5 TEU limits Union competences by reference to the principle of conferral. Article 4(1) TEU makes clear that competences not conferred on the Union remain with the Member States. These Treaty provisions are 'jurisdictional' in nature. They set out the scope – and limits – of EU law. They are not dealing with the manner in which conferred competence is exercised; but who has the competence.

14. Article 4(2) TEU makes clear that safeguarding national security is an essential State function. It emphasises explicitly that *"national security remains the sole responsibility of each Member State"*. In the context of provisions dealing with jurisdiction or competence, the choice is between competence being conferred on the EU by Member States, being shared between the EU and Member States or being retained by Member States and not conferred on the EU. The use of the word "*sole"* could not be clearer. Responsibility for national security lies with the Member States not the EU. It is not a competence conferred upon the Union in the Treaties.

15. The question is thus whether an activity is properly within the concept of "national security" for this purpose. In the present context, it is clear that the activities described above fall at the heart of Article 4(2) TEU – BCD is acquired and used by the Agencies for the protection of national security and the public.[5]

16. Article 4(2) is not a derogation. It is a foundational Treaty provision falling to be interpreted as such. That is confirmed by the International Law Decision of 18-19 February 2016 at section C.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*

[5] See also, OfR §36.

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."[6]

17. The effect of Article 4(2) was considered in *Remondis*, C-51/15, ECLI:EU:C:2016:985. That case concerned the issue of whether the definition of "*public contracts*" in the EU directive on public procurement extended to an agreement between two regional authorities to form a common special-purpose association with separate legal personality. The CJEU answered it by reference to Article 4(2) TEU, adopting the view of Advocate-General Mengozzi in his Opinion of 30 June 2016 (ECLI:EU:C:2016:504) that such matters fell outside the scope of EU law altogether. It is apparent that:

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

    (2) As acts of secondary legislation such as a directive must be in conformity with primary law (i.e. the Treaties), they cannot be interpreted as permitting interference in matters to which Article 4(2) TEU applies. Such matters remain outside the scope of EU law and, more specifically, EU rules set out in a directive: see the Opinion of AG Mengozzi at §§41-42, as endorsed by the CJEU in its Judgment at §§40-41. National security is quintessentially such a matter, as emphasised not only by the second sentence of Article 4(2) TEU but also the third sentence.

18. Consistently with this position, in Title V of Part Three of the TFEU (relating to the Area of Freedom, Security and Justice), it is confirmed that responsibility for national security remains with Member States, and is not conferred upon the EU: see Articles 73 and 276 TFEU. They make clear that the competence of Member States for the safeguarding of national security is unaffected and outside the scope of EU law,

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

notwithstanding that it remains open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate.

19. Thus, when (following the Lisbon Treaty) Article 16(2) TFEU provided for the EU legislature to make rules on the protection of personal data, it did so in terms that confined the power only to those activities of Member States which fall within the scope of EU law (underlining added):

> "*The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States 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.*"(emphasis added)

The inclusion of the underlined words expressly recognised that the Union's competence to make rules relating to data protection does not extend to activities that fall within the scope of Member States' competence such as those carried out to protect national security, consistently with Article 4(2).

Directives

20. That approach had already been incorporated in the text of Article 3(2) of Directive 95/46 ("**the Data Protection Directive**") which provides:

> *"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,…"* (emphasis added)

21. The effect of Article 3(2) of the Data Protection Directive has been considered in *Lindqvist,* C-101/01, EU:C:2003:596 at §43 and *Satakunnan Markkinapörssi,* C-73/07, EU:C:2008:727 at §41. In those cases, the CJEU confirmed that that by virtue of Article 3(2), the Data Protection Directive does not apply to the processing of personal data in the course of an activity that falls outside the scope of EU law such as those listed in Article 392.

22. The e-Privacy Directive translates the principles of the Data Protection Directive into specific rules in relation to electronic communications services. Article 1(3) of the e-Privacy Directive effectively replicates the terms of Article 3(2) of the Data Protection Directive and provides that the e-Privacy 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.*"[7]

23. Thus, each of the key Directives recognised the exclusion from the scope of the Directive of key activities that were not competences of the Union. In particular, matters of national i.e. State, security are specifically covered by the exclusion.

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

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

25. It is thus plain from those provisions that the EU legislature correctly recognised the scope of each of the Directives as limited to those activities falling outside the various identified areas.

26. In light of the primacy of Article 4(2) TEU and Article 16(2) TFEU, that was inevitable and was a necessary recognition in the case of essential State functions relating to national security. Competence in such matters has advisedly not been conferred upon the EU at all, but retained as the sole responsibility of Member States. It would be constitutionally impermissible for a Directive to make provision to the contrary.

27. It follows that the scope of the e-Privacy Directive does not and cannot extend to activities necessary in support of Member States' national security, including in particular the transfer of data, such as BCD, to Agencies and its use by them. Article 1(3) EPD appropriately excludes those activities from its scope. It must be given full effect, in light of the primacy of Article 4(2) TEU, and the absence of any competence of the EU to legislate on matters of Member States' national security.

II. *Watson* does not lead to any different conclusion to that evident from the clear words of Article 4(2)

28. The competence of Member States in relation to national security matters, as explicitly recognised in Article 4(2) TEU is unaffected by the Court's decision in *Watson.* That

[7] See also Recital (11) of the e-Privacy Directive.

decision was not directed towards the specific issue of the acquisition and use of data by the Agencies in the interests of national security, nor did it consider the particular importance of the role of Article 4(2) TEU.

(i) National security activities

29. In *Watson,* the CJEU recognised at §69 that Article 1(3) of the e-Privacy Directive excludes from its scope "*activities of the State*" in the areas of criminal law 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. The CJEU expressly drew an analogy with Article 3(2) of the Data Protection Directive.

30. At §70 of *Watson*, the CJEU contrasted the effect of Article 1(3) EPD with that of Article 3 EPD, which sets out where the directive does apply – namely, to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices ("***electronic communications services***"). In contrast to the position in *Watson,* the present case is concerned squarely with national security activities – including at the only stage at which providers of electronic communications services are involved, when required for national security reasons to transfer BCD to the Agencies.

31. It is therefore apparent that the CJEU drew a direct contrast between "*activities of the State*" falling within the specified fields on the one hand, which fall outside the scope of the e-Privacy Directive, and "*activities of the providers of electronic communications services*" on the other, to which the Directive directly applies.

32. Against that background, the CJEU considered the effect of Article 15(1) of the e-Privacy Directive at §§71-74. Notably, at §72, the CJEU noted the importance of the contrast between activities "*characteristic of States or State authorities*" and those which are "*unrelated to fields in which individuals are active*" (referring to Case C-275/06 *Promusicae*, which in turn referred back to *Lindqvist* at §43). It concluded at §74 that the legislative measures referred to in Article 15(1) governed "*the activity of providers of electronic communications services*" and not the activity of the State or of State authorities.

33. Its ensuing analysis clearly reflected that distinction. Thus, for example:

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

(2) At §76, the CJEU stated that the scope of the Directive also extended to a legislative measure relating to the access of the national authorities to the data retained *"by the providers of electronic communications services"*.

34. As already noted, here (and in contrast with the position in *Watson*) the providers of electronic communications services are involved only at the stage of transmission of the BCD. Two points are to be noted:

(1) In the case of the necessary acquisition of BCD there is inevitably the need for transmission by service providers when the data is first acquired by the Agencies. That data is acquired in order that the Agencies can undertake their national security functions.

(2) The fact that the transmission is pursuant to a legal requirement on the service providers rather than, hypothetically, by way of a physical extraction by state agencies, cannot in effect make all the legal difference. It does not alter the fundamental purpose of the data being acquired and retained: national security. The core issue of characterisation – whether the activity is properly characterised as within national security – must be answered in the same way, despite the minimal (and for present purposes, adventitious) involvement of the service provider in transmitting the BCD in this way. Moreover, to seek to use that involvement in effect to open up competence not merely in relation to transmission but also in relation to all the subsequent activities (including use of the BCD by the Agencies) cannot be permissible. It would cut across a faithful application of the clear division of competences in Article 4(2) in circumstances in which the activities in question are all plainly national security activities and the vast majority of them have nothing whatever to do with service provision.

35. Indeed, the Grand Chamber of this Court has already held that the transfer of personal data collected by private operators for commercial purposes to State authorities pursuant to national legislative requirement adopted in the interests of public security and the activities of the state in areas of criminal law, does not fall within the scope of EU law.

It is submitted that that approach was correct and faithful to Article 4(2)'s evident intention. It so held in *Parliament v Council*, Joined Cases C-317/04 and C-318/04, ECLI:EU:C:2006:346, at §59, when it decided that Commission Decision 2004/496 that adequate arrangements had been made for the protection of bulk PNR data (collected for airlines' commercial purposes) transferred to the United States authorities fell outside the scope of the Data Protection Directive. The reason was that the processing of such data "*falls within a framework established by the public authorities that relates to public security*": see §58. *A fortiori,* processing of data involved in activities such as the transfer of BCD to the Agencies for the purposes of national security does not fall within the scope of the Data Protection Directive (see Article 3(2) of the Data Protection Directive); nor equally can it engage the e-Privacy Directive (see Article 1(3)). Following the Lisbon Treaty, Article 4(2) TEU put this beyond doubt.

36. The Grand Chamber reaffirmed that conclusion in *Ireland v Parliament*, C-301/06, ECLI:EU:C:2009:68, a case which concerned the correctness of the legal basis for Directive 2006/24 ("**the Data Retention Directive**"). The Grand Chamber held that the provisions of the Data Retention Directive, which amended the e-Privacy Directive, were "*essentially limited to the activities of service providers"*, to the exclusion of State activities coming under Title VI of the TEU (as it then stood, dealing with police and judicial cooperation in criminal matters): §§80-84. As it explained at §88, in *Parliament v Council,* the Court had held that the subject-matter of the Commission's 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. In paragraphs 57 to 59 of the judgment in Parliament v Council and Commission, the Court held that such data-processing was covered by Article 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.*"

37. Thus, at §91, the Court distinguished the scope of the Decision from that of Directive 2006/24: the former "*concerned a transfer of personal data within a framework instituted by the public authorities in order to ensure public security",* whereas the Data Retention Directive, by contrast, "*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.*"

38. The present case falls firmly into the former category of case, not the latter. Just as was the case in relation to the PNR data considered in *Parliament v Council,*

communications data is collected by a private operator for commercial purposes. Where a section 94 direction has been issued to such an operator, that data is transferred to the Agencies (MI5 or GCHQ) within a framework established for national security. The data is not otherwise required to be retained by the PECN operators, and they do not do so for any other purpose beyond their ordinary, independent, commercial purposes (such as billing and fraud prevention).

39. The CJEU did not refer to or qualify this decision in *Watson*, despite the fact that the referring court (the Court of Appeal) had specifically drawn attention to it: see *Davis and ors v SSHD* [2015] EWCA Civ 1185 at (among other places) §§56-58 and 95-96.[8]

40. Finally, the fact that BCD acquired by the SIAs for national security purposes under a s.94 direction may be shared by the Agencies (pursuant to s.19(2), (3) and (5) of the Counter-Terrorism Act 2008), for use in the context of the activities of the State in the areas of the prevention and detection of serious crime of for criminal prosecutions, is not relevant. Plainly, after the acquisition of such data by the Agencies on national security grounds, its subsequent use for purposes which continue to fall outside the scope of the e-Privacy Directive, by virtue of Article 1(3), is outside the scope of EU law and the directive.

41. The result is that the use of BCD acquired under a section 94 direction falls outside the scope of the EPD. No other approach gives meaningful effect to Article 4(2) TEU; or to Article 1(3) EPD.[9]

(ii) National security rather than criminal investigation

42. As the Tribunal observed at §25 of the OfR, the first of the two joined cases (*Tele2 Sverige*) 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: see *Watson* §22. The UK legislation at issue ("**DRIPA**") provided for a retention notice requiring Public Networks 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 RIPA: see *Watson* §29. Although those purposes included *inter alia* national security, they were not so limited: in particular, retention notices could be issued for the purpose of preventing or detecting crime or of preventing disorder,

[8] http://www.bailii.org/ew/cases/EWCA/Civ/2015/1185 html
[9] See also OfR §36.

without being expressly limited to "serious crime". (Retention notices could also be issued for other purposes, including the economic well-being of the United Kingdom, the interests of public safety or protection of public health, for assessing or collecting taxes, and any other purpose which may be specified by an order made by the Secretary of State.)

43. The Court reached its conclusions by reference to the investigation of crime, and not national security.

44. The sole exception to that position is the short passage in one paragraph of the judgment, §119, which refers (indirectly) to the ability to grant competent national authorities access not 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; but also to that of other persons "*in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities*", and 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.

45. It is submitted that this cannot be taken as a finding by the Court that the acquisition and use of BCD by the Agencies to identify previously unknown threats to national security falls within the scope of EU law. The passage did not form any part of the Court's analysis on the question of scope. Neither Article 4(2) TEU nor Article 1(3) EPD was considered in this context. Nor does national security play any part in the *dispositif* – with good reason, as it falls out of scope of EU law, was not raised in the questions referred to the Court, and played no substantive part in the Court's reasoning. Unsurprisingly, therefore, the Court did not analyse national security activities, which include nuclear counter-proliferation, defence against cyber-attacks from a hostile state, support of troops in an armed conflict abroad, counter-espionage, or counter-terrorism in its national security aspect (rather than purely criminal aspect). In any event, the Court did not have anything close to the careful, detailed focus on the relevant issues that is provided in the OfR and the parties' submissions on it.

(iii) Role of Article 15(1)

46. Article 15(1) EPD includes reference to "national security". However, that cannot be taken to override Article 1(3) EPD, and still less Article 4(2) TEU given the primacy of

the Treaties. The effect of Article 4(2) TEU, reflected properly in Article 1(3) EPD, is to create an exemption from the scope of EU law and of the EPD in particular – not to provide for a derogation. As already noted, it would be constitutionally impermissible for a provision in a Directive to purport to create competence where none exists under the TEU. Thus, the inclusion of such wording in Article 15(1), in the context of a provision which otherwise appears to refer to grounds for derogation, is incapable of bringing within scope of the Directive matters of Member State responsibility which are plainly intended to be excluded from the scope of EU law altogether.

47. To that extent, the Court's observation in §73 of *Watson* that 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 the directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met"* cannot be applied in the context of activities in the field of national security. Article 1(3) cannot be "*deprived of any purpose*" any more than can Article 15(1).

48. In any event, the Court noted at §74 that "*the legislative measures referred to in Article 15(1) govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services.*" Article 15(1) plainly does not refer to legislative measures which govern the activities of the State authorities concerning national security, or any other activities which are so closely connected with the State's activities that they form part of the national security framework. In each case, those matters fall outside the scope of the Directive by virtue of Article 1(3) (and Article 4(2) TEU), with the result that Article 15(1) can have no application to them. Just as the Court recognised that the activities of State authorities in the area of criminal law remained out of scope of the Directive notwithstanding the terms of Article 15(1) (see §69), the same is true of activities falling within the national security framework.[10] While the criminal exclusion in Article 1(3) is specifically limited to 'activities of the State', the exclusion for national security is not limited in those terms. This is unsurprising in circumstances where (as outlined above) the ability of a State to protect its national security is heavily dependent on data from other sources. To conclude otherwise would seriously undermine Member States' ability to protect their national security.

[10] Were it otherwise, the reference to "national security" in Article 15(1) would be *ultra vires.*

49. Finally on this aspect, insofar as there remains any conflict between Article 1(3) and 15(1), the Tribunal identified the appropriate way to reconcile this position at §§37-39 of the OfR.

III. *Commission v Italy* and *ZZ (France)* do not assist the Claimant

50. The Claimant further relies on two cases to support its proposition that s.94 directions fall within the scope of EU law, even if they are outside the scope of the e-Privacy Directive and notwithstanding that they are made in the interests of national security: see OfR §31, where the Tribunal refers to the Claimant's reliance on *Commission v Italian Republic,* C-387/05, ECLI:EU:C:2009:781, at §45, and *ZZ (France)*, C-300/11, ECLI:EU:C:2013:363, at §38.

51. Neither case is analogous to the present one.

(1) In *Commission v Italian Republic*, the Italian Republic had sought to derogate from a Treaty obligation for the charging of common customs duties by exempting imports of material capable of use both for civil and military purposes. It did so claiming that such a derogation was justified on the grounds of the protection of the essential interests of the security of the Member States, without adducing any evidence in support of that position. The Court rejected that submission on the grounds that there was no inherent general exception excluding all measures taken for reasons of public security from the scope of Community law, that the derogations provided for under the Treaty must be interpreted strictly, and that it was consequently for a Member State which sought to take advantage of such a derogation to prove that it was necessary to have recourse to it to protect its essential security interests. The Italian Government had not done so.

(2) In *ZZ (France),* the Italian Government objected to the admissibility of a request for a preliminary ruling concerning Article 30(2) of Directive 2004/38, read in the light of Article 47 of the Charter. The Secretary of State's decision to exclude ZZ, an EU citizen, from the United Kingdom had relied upon the public security derogation in Article 30(2) of the Directive. The Italian Government argued that it was clear from Article 4(2) TEU and Article 346(1)(a) TFEU that State security remained the responsibility solely of the Member States. The Court cited *Commission v Italian Republic* for the proposition that 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. But it did so in the particular context that the United Kingdom was explicitly seeking to derogate from ZZ's right of freedom of movement under the Treaty on grounds of public security.

52. In each case, the argument advanced was that a Member State was free to *derogate* from a Treaty obligation on the grounds that it had asserted that its decision to do so was based upon its essential security interests. Unsurprisingly, in each case the argument was rejected. The present case is different, however: the United Kingdom is not seeking to justify any derogation from a Treaty obligation or any other rule of EU law. No such derogation is necessary, because there is no relevant right engaged. To the contrary, there is express provision in Article 1(3) of the e-Privacy Directive itself, interpreted consistently with primary law in Article 4(2) TEU, which makes clear that the rights conferred by the EPD do not extend to activities which fall outside the scope of the Treaty (which includes national security activities). There is therefore nothing within the scope of EU law from which the United Kingdom is required to derogate.

IV. Conclusion on Question 1

53. For the reasons set out above, and as appears at paragraph 35 of the Order for Reference, it follows that:

(1) The exercise of a legal power by the government of a Member State to require a PECN operator to transfer data to the State in order to protect national security is an activity of the State not within the scope of EU law.

(2) The activity of the State in making use of the transferred data for the purpose of protecting national security is not within the scope of EU law.

(3) The activities of commercial undertakings in processing and transferring data to the Agencies for such purposes, as required by national law, also falls outside the scope of EU law.

QUESTION 2

54. In view of the answer to the Tribunal's first question, the second question does not arise for consideration. However, if the second question were to arise, the answer to it would be in the negative. The safeguards identified in the context of the data retention regime considered in *Watson* cannot be read across and applied here in the current context. The imposition of the *Watson* requirements would not reflect a proportionate balance between any interference with rights under Article 7 and 8 of the Charter and the objective of protecting national security, and the rights and freedoms of others. It would seriously put the safety of the public at risk, in circumstances in which adequate and effective safeguards, compatible with the ECHR, already exist in the domestic legal regime. There is no warrant for EU law to impose requirements well above and beyond those considered adequate under the ECHR in such circumstances. The European Court of Human Rights has repeatedly emphasised that running through the scheme of Convention rights is a balance between private rights and freedoms and the general interests of the community. The same must be true, and is recognised, in the context of the Charter. It is submitted that the balance cannot properly be struck, so as to insist upon requirements beyond the ECHR at the expense of critically undermining a State's ability to protect its citizens.

I. The acquisition and use of BCD is necessary and appropriate to protect national security

55. The Agencies' capabilities to acquire and use BCD are essential to their ability to protect national security and thus the public. This was one of the key findings of fact made by the Tribunal (see §§10-16 and 59(i)-(ii) of the OfR); and provides one of the factual bases for this Reference.

II. There are extensive safeguards in place in respect of the use of BCD by the Agencies

56. The existing safeguards in place under the domestic legal regime are already sufficient to prevent abuse and protect against arbitrary use of the powers, and in particular fully to comply with the requirements of the ECHR (including that any interference with privacy rights be "*in accordance with the law*").

57. The existing safeguards were extensively considered by the Tribunal in its judgment of 17 October 2016 (which accompanies the Order for Reference) ("**the October judgment**"). It listed in Appendix A of the October judgment the key features of the statutory framework and safeguards which surrounding the BCD regime. The totality of those safeguards need to be taken into account in considering the present issue. However, in the briefest summary:

(1) The Agencies' functions are prescribed by statute, and the use of the BCD capabilities in particular must at all times be consistent with various legislation, including the Counter-Terrorism Act 2008, the Human Rights Act 1998, the Data Protection Act 1998, and the Official Secrets Act 1989.

(2) Mandatory handling arrangements are applied, including detailed provisions as to the necessity and proportionality of acquisition, access/use and disclosure. There are further requirements to undertake regular formal reviews of the justification for continued retention and use for the consideration of the relevant Secretary of State. Internal audit teams must monitor and report to detect any misuse, and reports on audit investigations are made to the Commissioner (see below).

(3) The operation of the regime is subject to effective external oversight. The Investigatory Powers Commissioner is responsible for keeping under review and overseeing the acquisition, use and disclosure of communications data by the Agencies. (Prior to September 2017 such oversight was provided by the Interception of Communications Commissioner.) The Commissioner, Lord Justice Sir Adrian Fulford, is (like his predecessors) an eminent and very senior judge. He can call for all such documents and information as he may require from the Secretary of State and the Agencies to enable him to exercise that oversight. He is also required by statute to give the Tribunal such assistance as the Tribunal may require in investigating and determining complaints.

(4) The Tribunal has broad jurisdiction to consider complaints about the Agencies' activities. Its functions and approach are described in detail in the October judgment. It is an important part of the external oversight regime.

58. The Tribunal fully analysed these safeguards, with the benefit of extensive evidence as to their application in practice. It concluded that, since the arrangements were publicly "avowed", the BCD safeguarding regime has complied with the requirements of Article

8 ECHR. The safeguarding standards imposed by the ECHR are, as it found, rigorous. The Tribunal was satisfied that the following principles which it derived from the ECHR case law (see §62 of the October judgment) were met:

(1) There must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action. It must be satisfied that there exist adequate and effective guarantees against abuse.

(2) The nature of the rules fettering such discretion and laying down safeguards must be clear and the ambit of them must be in the public domain so far as possible; there must be an adequate indication or signposting, so that the existence of interference with privacy may in general terms be foreseeable.

(3) Foreseeability is only expected to a degree that is reasonable in the circumstances, being in particular the circumstances of national security, and the foreseeability requirement cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures, so that he can adapt his conduct accordingly.

(4) It is not necessary for the detailed procedures and conditions which are to be observed to be incorporated in rules of substantive law.

(5) It is permissible for the Tribunal to consider rules, requirements or arrangements which are 'below the waterline' i.e. which are not publicly accessible, provided that what is disclosed sufficiently indicates the scope of the discretion and the manner of its exercise.

(6) The degree and effectiveness of the supervision or oversight of the executive by independent Commissioners is of great importance, and can, for example in such a case as *Kennedy v UK* [2011] EHRR 4, be a decisive factor.

(7) There must be adequate arrangements in place to ensure compliance with the statutory framework and the ECHR and to give the individual adequate protection against arbitrary interference, which are sufficiently accessible, bearing in mind the requirements of national security and that they are subject to oversight.

59. Moreover, even if the effect of Article 4(2) is not as already submitted, it nevertheless has real significance to the approach to safeguards and proportionality. In the context of national security, the effect of Article 4(2) TEU is at the least that a Member State has

the broadest possible margin of discretion to judge what is necessary and proportionate in the interests of national security. Given that national security remains the "*sole responsibility*" of each Member State, only the Member State is in a position to assess the seriousness of the threats that it faces, and hence the necessity of using bulk data to assist in averting those threats, in particular by identifying the individuals who present them. Moreover, it cannot be appropriate or permissible to seek to impose safeguards which would critically undermine the ability to protect national security. All of this is inconsistent with the imposition under EU law of prescriptive safeguards which are not apt to the circumstances of the present case.

III. The level of interference with the rights in Article 7 and 8 of the Charter is low, and substantially lower than the use of alternatives (where they exist at all)

60. The level of interference with the rights in Articles 7 and 8 of the Charter arising from the operation of the BCD regime should not be overstated. As the Tribunal found,[11] alternatives to the use of BCD would not be able to provide the same protections of national security and, to the extent they might be used to substitute for the use of BCD, they would be not only less effective but would lead to *more* intrusive interference with the right to respect for private life than is involved by the Agencies' use of BCD.

61. Moreover, whatever adjective is applied to describe the interference, the important point is a relative one: the nature of any interference is to be viewed relative to the legitimate aim sought to be achieved by the interference – here the protection of the lives and safety of the public through the protection of national security (a matter reflected in Article 6 of the Charter) – and having regard to the overall balance running through the Charter (just as through the ECHR) between private rights and freedoms and the general interests of the community.

62. As the Tribunal explains at §16 of its Order for Reference, the BCD capabilities are <u>not</u> used 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 <u>minimal</u> intrusion, to obtain access only to the data of persons whose activities may constitute a threat to national security. Thus a suspected potential Al-Qaeda suicide bomber was able to be identified from a bulk dataset, applying computer filters and matches to a pool of

[11] See OfR §§10-17.

27,000 candidates. Without this capability, it would be necessary to carry out other and more intrusive enquiries, or to use other more intrusive powers in order to narrow the scope of a search.

IV. The *Watson* requirements cannot be read across to this context

63. In *Watson,* the CJEU identified safeguards at §§119 to 122 which it considered were – or at least might be – appropriate to the circumstances of the targeted investigation of serious crime. The *Watson* requirements were applied in respect of the targeted use of communications data. The Court did not consider, or rule on, the appropriate safeguards applicable in a national security context such as the present one.

64. The *Watson* safeguards cannot be applied to the Agencies' acquisition and use of BCD without critically undermining the ability of the Agencies' ability to tackle threats to national security. As already noted, that was also one of the central findings of fact made by the Tribunal; and is thus a fundamental premise on the basis of which these issues are to be considered by the Court. The Tribunal has considered the effect of the imposition of the *Watson* requirements in relation to the BCD regime, and has found them to be wholly unsuitable in this context.

65. Access to BCD acquired under a s.94 direction is not properly comparable to the Swedish legislation or the DRIPA regime considered in *Watson*. There are (at least) four important differences.

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

67. **Second**, under each of the relevant data retention regimes considered in *Watson,* the service providers were required to retain data for which they had no further commercial use. The sole purpose of retention was to ensure that data that would not otherwise be held by a CSP for business purposes is available to be accessed and disclosed to the authorities on request. That is not the position in the BCD regime.

68. **Third**, so far as BCD acquired under a s.94 direction is concerned, the data omits subscriber information, distinguishing the position from that described in *Watson* at §98. (Subscriber information data must be obtained separately.)

69. **Fourth**, in *Watson*, the court focused in particular on the particular question of the proportionality of providing access to retained data in relation to the objective of fighting crime, even though it recognised that other objectives were also permissible: §§115, 119. The CJEU did not address the question of the proportionality of access to retained data in other circumstances:

    (1) Even where, at §119, the CJEU recognised that national security, defence or public security interests could be threatened, justifying greater access than it thought might otherwise be proportionate, it still did so in the context of "*particular situations*" including the prevention, investigation, detection or prosecution of specific cases of criminal (terrorist) activity.

    (2) The CJEU has not addressed the proportionality of access to retained data for other national security purposes, for example, in the context of the fight against nuclear proliferation, counter-espionage, defence against cyber-attacks by a foreign state, or military conflicts threatening the geo-political security of Member States of the EU (such as events in Ukraine or Syria).

70. The Claimant's insistence on the application of the *Watson* requirements would as the Tribunal has found critically undermine the protection of national security. That fact, coupled with the existence and ECHR compliant nature of the domestic safeguarding regime in the present context, indicates that that insistence would fail to strike a proportionate balance between the privacy of individual users of PECNs and the public interest in the effective protection of national security.

(a) Targeted access

71. As to the requirement for targeted access only, such a requirement is incompatible with both the main purpose of holding BCD (to discover previously unknown threats), and the means by which the BCD database is used (by using automated filters and matches). As set out above and as found by the Tribunal at §44, it is not possible to limit the use of the database to "particular situations", as referred to in §119 of *Watson;* nor is it possible to await "objective evidence" from which it may be deduced that the "data of other persons" might "in a specific case" be of use – the aim is to pre-empt threats; threats which evolve both in their methodologies and form. Nor is it possible to limit the acquisition of BCD to certain geographic areas, which is impracticable when dealing with international terrorism, or threats to national security arising from espionage or nuclear proliferation activities.

72. In fact, the Claimant is wrong to insist upon the dogmatic application of any such requirements, without regard to the context in which they would have to be operated. Thus, in Opinion 1/15, AG Mengozzi recognised at §205, §§215-216, §241 and §244 that a different approach to safeguards than that adopted in *Digital Rights Ireland* and *Schrems* was appropriate in the case of the provision of bulk PNR data to the Canadian authorities, in light of the different nature of the activity and the purpose of threat identification served. The difference in nature and purpose of the data was relied upon by the Advocate General to explain why safeguards thought applicable in the context of the Data Retention Directive in *Digital Rights Ireland* (and subsequently to national measures in *Watson*) did not apply in the same way.

73. Similarly, in its Opinion of 26 July 2017 at §§186-187, the Court recognised that it would be inappropriate to transfer only PNR data to Canada if there was already objective evidence permitting the inference that the passengers were liable to present a risk to public security in Canada, or to confine such transfer of data to certain categories of persons or certain areas of origin, which would prevent the achievement of the objective of automated processing of PNR data – i.e. identifying persons liable to present a risk to public security from amongst all air passengers. In so recognising, it is apparent that the *Watson* requirements are not inflexible rules of principle, but are sensitive to context and should be applied only where it is appropriate to do so.

(b) Prior independent authorisation

74. Secondly, a requirement of prior independent authorisation before accessing data "*would critically undermine the ability of the SIAs to tackle some threats to national security*" (Order for Reference, §48). In the context of the transfer of PNR records to Canada, Advocate General Mengozzi recognised at §269 of his Opinion that such a requirement was unnecessary in that context. The Court agreed at §197 of its Opinion. Although the Court held that, except in cases of validly established urgency, such prior authorisation would be required in respect of subsequent use of that data (at §202), this reinforces the point that the need for such authorisation is sensitive to context and to practicability.

75. The Tribunal considered the practicability of such a requirement in the present context, and found that it would not be practicable without critically undermining the ability of the Agencies to tackle some threats to national security. There is no basis upon which to depart from this factual finding, reached by the specialist national court on the basis of an extensive review of the evidence.

(c) Notification

76. For the reasons explained by the Tribunal at §§49-51 of the Order for Reference, a requirement of notification of those affected is impractical and damaging to national security. The process of building intelligence on threats to national security is always ongoing. At no point does it become safe to notify individuals who have been investigated that their data has been accessed: as the Tribunal explained: "*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."*

77. Although the Court found in Opinion 1/15 (at §220) that such notification would be appropriate in the context of the EU-Canada agreement, that agreement was justified on the grounds of the fight against terrorism and serious transnational crime. However, additional matters arise in the context of national security, rendering the data retention safeguards identified in *Watson* clearly inappropriate in that context. In particular, the work of the security and intelligence agencies must be conducted in secret if it is to be effective in achieving its aims. The value of intelligence work often relies on an identified target not knowing that his activities have come to the attention of the

agencies, and/or not knowing what level of access to his activities the agencies have achieved. The requirement to notify a suspect of the use of bulk data tools against him, simply on the grounds that investigations have been concluded, would fundamentally undermine the work of the agencies.

78. In those circumstances, the Tribunal concluded (at §50) that to impose such a requirement would be "*very damaging to national security*". It noted that, in the United Kingdom, there is already an effective remedy before a tribunal: the Investigatory Powers Tribunal is itself able to examine a complaint by any person who fears or suspects that their data may have been accessed unlawfully, without involving disclosure of any information contrary to the interests of national security. Through the use of developed techniques of deciding complaints on "assumed facts", and with the benefit of access to classified material, the rights of any concerned individuals are protected (as the ECtHR concluded in *Kennedy v UK*).

79. In those circumstances, in particular having regard to the adequacy of existing safeguards in the United Kingdom, it is inappropriate and unnecessary to impose a requirement of notification.

(d) Retention of data in the EU

80. There can be no absolute bar on the transfer of data out of the EU, and the United Kingdom does not understand the CJEU to have suggested otherwise in *Watson*: the Court was not dealing with the issue of the ability of States to transfer data outside the EU, and it cannot be suggested that retention of data within the EU is an unconditional mandatory requirement of EU law. The ability to share such data between the State authorities responsible for national security cannot be so restricted in the context of threats such as international terrorism, espionage by hostile powers, and nuclear proliferation.

81. A requirement that the PNR data be kept within the EU was obviously inapplicable in Opinion 1/15. To the contrary, the whole purpose of the agreement was to allow for the appropriate sharing of the data outside the EU. There is no suggestion that such transfer is antithetical to EU law in principle. That is unsurprising: §122 in *Watson* is concerned with the security and protection of data retained by providers of electronic communications services, not with the use of such data once it has been accessed or acquired by the national authorities. Those uses must inevitably be international in

nature, given the international threat to national security and the need to liaise closely with other trusted countries' intelligence services in order to meet that threat.

V. Conclusion on the second referred question

82. The second question should accordingly be answered in the negative.

PROPOSED ANSWERS TO BE GIVEN TO THE REFERRING COURT IN RELATION TO THE QUESTIONS REFERRED

1. A direction by a Secretary of State to a provider of an electronic communications network that it is necessary and proportionate for it to provide bulk communications data to the Security and Intelligence Agencies of a Member State in the interests of national security does not fall within the scope of Union law or of the e-Privacy Directive in particular.

If it is necessary to answer the second question:

2. Neither the "*Watson Requirements*" referred to at paragraph 40 of the Order for Reference, nor any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State.

Simon Brandon

[redacted]

Agent for the United Kingdom

Daniel Beard QC

Robert Palmer

Barristers