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

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

CLAIMANT'S OUTLINE OF EU LAW SUBMISSIONS

for the hearing from 8 to 10 March 2017

---

1. This is the Claimant's response to a request by the Respondents for it provide an outline of its intended submissions in relation to the issues of EU law that arise for determination by the Tribunal. The Claimant reserves its right to develop its grounds of claim, in particular following disclosure by the Respondents.

Section 94 Regime

2. A direction under section 94 of the Telecommunications Act 1984 to a CSP ('**TA 1984**') engages EU law:

   2.1. Article 5 of the Directive 2002/58/EC (the '**e-Privacy Directive**') requires that the confidentiality of telecommunications be ensured *except* when access is legally authorised in accordance with Article 15(1).

   2.2. The CJEU in C-698/15 *Watson & ors* ('***Watson***') held that a retention notice issued under section 1 of the Data Retention and Investigatory Powers Act 2014 ('**DRIPA**') fell within the scope of the e-Privacy Directive; see §§ 70-81 of *Watson*. At § 73 of *Watson*, the CJEU held:

> *Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within*

the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.

2.3. A direction under section 94 of the TA 1984, imposing retention, processing and delivery requirements on a commercial telecommunications provider in relation to bulk communications data ('BCD'), is materially identical to a DRIPA retention notice for these purposes. It therefore falls equally within the scope of the e-Privacy Directive.

3. Large-scale bulk retention of communications data is unlawful under EU law. See *Watson* §§ 89, 96, 97, 99-101 and 107.

4. In any event, the Section 94 Regime does not contain any of the necessary safeguards on access to data:

4.1. "*it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime*": *Watson*, § 120.

4.2. "*the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities*": *Watson*, § 121.

4.3. "*the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period*": *Watson*, § 122.

5. The statutory scheme under s. 94 of the TA 1984 does not contain any of the safeguards referred to above; it therefore permits interference with privacy and confidentiality rights that is unnecessary and disproportionate:

5.1. There is universal mass retention of communications data.

5.2. There is no mechanism to ensure that BCD acquired under s. 94 of the TA 1984 is used only for the purpose of fighting serious crime.

5.3. There is no requirement for prior independent authorisation for access.

5.4. There are no procedures for notification of use of the data.

5.5. There are no adequate controls on how BCD acquired under s. 94 of the TA 1984 is shared.

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

6. The above principles of EU law are well-established and ought to be given effect promptly by the Tribunal.

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

BPD Regime

8. The obtaining of BPDs engages EU law pursuant to Directive 95/46/EC ("**the Data Protection Directive**").

9. Where the information contained in a BPD is of a broadly equivalent level of intrusiveness to communications data, the principles of necessity and proportionality will require an equivalent level of safeguards governing access to data as those identified in *Watson*. See the opinion of Advocate General Mengozzi in *Opinion 1/15* concerning the EU-Canada draft agreement on the transfer and processing of Passenger Name Record Data.

10. Pending disclosure, such datasets are likely to include:

10.1. BPDs containing intercept material (it has been avowed that "*some BPDs are obtained by interception*" – David Anderson QC *Bulk Powers Review,* footnote 119).

10.2. health datasets (the Agencies have said that they do not currently retain such datasets, although they presumably might do so in the future);

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

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

10.5. any BPDs containing privileged material or identifying journalistic sources.

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

11.1. There is mass retention of BPD.

11.2. There is no mechanism to ensure that BPD are used only for the purpose of fighting serious crime.

11.3. There is no requirement for prior independent authorisation for access.

11.4. There are no procedures for notification of use of the data.

11.5. There are no adequate controls on how BPD acquired are shared.

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

Disclosure

12. The Tribunal has power to order disclosure of documents to a Claimant contrary to the wishes of a Respondent (see *Dias & Matthews v CC of Cleveland Police* [2017] UKIPTrib15_586-CH, Sir Michael Burton (President), Edis J, Mr Charles Flint QC, Professor Graham Zellick QC and Sir Richard McLaughlin) (*"This application for disclosure was resisted by the Respondent and granted by the Tribunal… what was produced was plainly inconsistent with the narrative statement…* [26-27]).

13. This recent decision confirms (a) the Tribunal's power to order disclosure; and (b) the importance of that power to securing a fair hearing. Rule 6(2)(c) of the IPT Rules 2000 is *ultra vires* to the extent it purports to provide the Respondents with a veto on disclosure.

14. Further, and in any event, the Tribunal has the following duties under EU law in relation to disclosure:

14.1. A duty to consider for itself whether disclosure should be given ("*it is necessary for a court to be entrusted with verifying whether those reasons stand in the way of precise and full disclosure of the grounds on which the decision in question is based and of the related evidence*" Case C-300/11 *ZZ v Secretary of State for the Home Department (Grand Chamber)* at [60]).

14.2. If disclosure cannot be given for reasons of national security, the Tribunal must nevertheless disclose "*the essence of the grounds which constitute the basis of the decision...*" *ZZ* [68]. There is a duty under EU law to provide a core irreducible minimum of disclosure to enable the Claimant effectively to challenge the retention of information in BCD and BPD relating to it.

THOMAS DE LA MARE QC

BEN JAFFEY

DANIEL CASHMAN

Blackstone Chambers

9 February 2017

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

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

Respondents

CLAIMANT'S OUTLINE OF EU LAW SUBMISSIONS

for the hearing from 8 to 10 March 2017

Privacy International
62 Britton Street
London
EC1M 5UY

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

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

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

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

Respondents

RESPONDENTS' OUTLINE RESPONSE
TO CLAIMANT'S EU LAW SUBMISSIONS

---

1. This is the Respondents' outline response to the Claimant's outline of its intended submissions in relation to the issues of EU law that arise for determination by the Tribunal. The Respondents will develop their response in their skeleton.

Section 94 Regime

2. A direction under s.94 of the Telecommunications Act 1984 to a CSP ("**TA 1984**"), which may be made on the basis that it is "necessary in the interests of national security", does not fall within the scope of EU law.

   2.1. Under Article 4(2) TEU, national security remains the sole responsibility of each Member State. Competence in this field has been reserved to the Member States and is not conferred upon the EU: see Article 4(1) TEU.

2.2. A direction under s.94 of the TA 1984 does not fall within the scope of Directive 2002/58/EC (the "**e-Privacy Directive**"). Article 1(3) of the e-Privacy Directive provides that it "*shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.*"

2.3. The reasoning of the CJEU in C-698/15 *Watson & ors ("**Watson**")* at §73 does not apply in the case of national security as referred to in Article 4(2) TEU.

2.4. A direction under s.94 of the TA 1984 is not to be treated for these purposes as analogous to a retention notice made under the Data Retention and Investigatory Powers Act 2014 ("**DRIPA**").

3. Alternatively, if a direction under s.94 TA 1984 does fall within the scope of EU law, the effect of Article 4(2) TEU is that Member States have the broadest possible area of discretion in operating in the field of national security, including in designing systems for collecting, retaining and accessing data. The consequence is that the CJEU's assessment of the proportionality of retention of and access to data pursuant to retention notices issued under s.1 of DRIPA in *Watson* cannot be read across to data collected, retained and accessed specifically because it is necessary in the interests of national security.

4. Further or alternatively, even disregarding the effect of Article 4(2) TEU, *Watson* cannot be read over into the context of a direction under s.94 TA 1984. An analysis of the necessity and proportionality of the collection, retention and accessing of data in the interests of national security yields different answers to those arrived at by the CJEU in *Watson*. In particular:

4.1. The collection and retention of data under a s.94 direction in the interests of national security does not amount to the unlawful retention of data for the reasons set out by the CJEU in *Watson* at §§ 89, 96, 97, 99-101 and 107. The acquisition of communications data in the present context is materially different from the issue of data retention as considered by the CJEU.

4.2. The CJEU's finding at §102 of *Watson* that the measure in issue (which had been introduced "*for the purpose of fighting crime*") was capable of being justified only by the objective of fighting "*serious*" crime, cannot be read as suggesting that the collection, retention and accessing of data cannot be justified in the interests of national security.

4.3. The safeguards referred to at §4 of the Claimant's outline submissions cannot sensibly or appropriately be applied to the accessing of data obtained under a s.94 direction in the interests of national security, and cannot be required to be applied to such data before such access could be held to be necessary and proportionate. Separate, extensive and carefully considered safeguards operate in view of the different powers being exercised and the different considerations which arise in the case of national security, including specifically intelligence organisations' activities.

5. The Claimant is accordingly incorrect to suggest that the findings of the CJEU in the context of *Watson* can be treated as "*well-established principles of EU law*" which can simply be read across and applied in the context of national security generally, and in the context of s.94 directions in particular.

6. The section 94 regime is not unlawful for the reasons advanced by the Claimant in relation to the ECHR. It is prescribed by law and does not amount to a disproportionate interference with fundamental rights.

BPD regime

7. The obtaining of BPDs in the interests of national security including specifically by the Security and Intelligence Agencies does not fall within the scope of EU law.

7.1. Under Article 4(2) TEU, national security remains the sole responsibility of each Member State.

7.2. The obtaining of BPDs does not fall within the scope of Directive 95/46/EC (the "**Data Protection Directive**"). Article 3(2) of the Data Protection Directive provides that it "*shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those*

provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law."

8. Alternatively, if the BPD regime falls within the scope of EU law, the effect of Article 4(2) TEU is that Member States have the broadest possible area of discretion in operating in the field of national security, including in designing systems for collecting, retaining and accessing BPDs. The consequence is that the CJEU's assessment of the proportionality of retention of and access to data pursuant to retention notices issued under s.1 of DRIPA in *Watson* cannot be read across to the BPD regime.

9. Further or alternatively, even disregarding the effect of Article 4(2) TEU, *Watson* cannot be read over into the context of the BPD regime. An analysis of the necessity and proportionality of the collection, retention and accessing of BPDs yields different answers to those arrived at by the CJEU in *Watson*, for similar reasons as those set out above under §4 above in relation to s.94 directions.

Disclosure

10. The Claimant does not explain the context in which the outline submissions on disclosure are made. Without prejudice to the Respondents' right to respond further when the context of the submissions made is apparent, the Respondents reply as follows:

    10.1. The Respondents will make submissions about the powers of the Tribunal under the Rules if it becomes necessary to do so in the context of this case.

    10.2. The nature and reach of the principles established by the CJEU in *ZZ* were considered and analysed both by the Court of Appeal in *ZZ* [2014] QB 820 and, more recently, by the Court of Appeal in *R (AZ Syria)* [2017] EWCA Civ 35. The 'essence of the grounds' disclosure principle applies depending on the context. It is not an absolute principle applicable whenever EU law might be said to be, or is, engaged. The question whether the principle is applicable depends on a range of matters including in particular the nature and seriousness of the right

interfered with, as *AZ Syria* establishes. On the basis of the principles set out in *AZ Syria*, the principle is not applicable in the present context.

JAMES EADIE Q.C.

ROBERT PALMER

17 February 2017