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

CLAIMANT'S REPLY NOTE
for hearing commencing 5 June 2017

---

1. This short note responds to new points raised in the Respondents' skeleton argument, which is the first occasion on which the Respondents have explained their case on EU law in any detail. Submissions already made in the Claimant's skeleton are not repeated.

Engagement of EU law

Amendment of section 94 TA 1984 on introduction of EU Common Regulatory Framework

2. In 2003, section 94 was amended to insert a requirement of proportionality. The changes were effected by Schedule 17 of the Communications Act 2003. The purpose of the 2003 Act was to implement the EU common regulatory framework for telecommunications in the UK. The explanatory notes to Schedule 17 state *"Schedule 17 contain[s] a large number of amendments to the existing law on wireless telegraphy, mainly for the purpose of implementing the new Directives"* [SA2/Tab 50].

3. The suggestion in the Respondents' skeleton that "*the requirement of proportionality was inserted to reflect the requirements of the ECHR*" is incorrect [Respondents' Skeleton §24]. The Human Rights Act 1998 came into force on 2 October 2000, the same date as RIPA was brought into force. The amendment to section 94 was made 3 years later, to ensure compliance with the new requirements of the common regulatory framework under EU law. Schedule 17 paragraphs 63-75 of the Communications Act 2003 made a number of changes to the Telecommunications Act 1984, repealing much of it. Section 94 was amended so that its terminology ("PECN" rather than "*public telecommunications operator*") reflected that used in the CRF (and thus in the Communications Act 2003); more significantly, the language of "*requisite or expedient*" in section 94(1) was replaced with "*necessary*"; and an overarching proportionality test was inserted in section 94(2A). Such changes were plainly made to give effect to the CRF, Article 15 of the E-Privacy Directive in particular whose express language is deliberately copied over into section 94(1) and (2A).

4. Every pointer is thus to such changes being made to comply with EU law, in recognition that use of section 94 to compel a PECN to do any particular thing would engage EU law, especially if section 94 was to be used (as in fact it was) as a species of warranting power. If the change was thought necessary to comply with the ECHR, the relevant changes would have been made in 2000, alongside RIPA. The fact the change was made in 2003 indicates that Parliament well understood that a section 94 direction to a PECN in a pure national security context would engage EU law if used to alter the PECN's obligations under the e-Privacy Directive and so would have to meet the proportionality standard in Article 15(1) of the e-Privacy Directive.

5. The same point is confirmed by the UK's faithful implementation of the amendment to Article 15 of the e-Privacy Directive to insert Article 15(1b) [A5/7]. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) give effect to Article 15(1b) by requiring communication providers to establish and maintain internal procedures for responding to requests for access to data. The Explanatory Note to the SI inserting this provision (SI 2011/1208) confirm that when so acting, the UK was implementing EU law, and the purpose was "*to allow police and the*

security service *to have access to personal data*". This is all entirely inconsistent with the notion that where a commercial communications service provider processes personal data for national security purposes, this is outside the scope of EU law.

UK's oral submissions to CJEU in Watson

6. The Claimant has served the Third Witness Statement of Millie Graham Wood, exhibiting a transcript of the UK's submissions to the CJEU in *Watson*. The transcript was made by Ms Graham Wood from the official recording of proceedings.

7. The transcripts confirm that the submissions now made to the Tribunal (e.g. as to the supposed effect of Article 4(2) TEU and Article 1(3) of the e-Privacy Directive) were squarely before the Court:

a) First, Mr Beard QC emphasised that the interference with privacy involved in data retention was more modest than a requirement (as with BCD) to "*give it to us, or to someone else*". Nor was there any "*wholesale sweep up of data by the investigating authorities… not a general database access*" (p. 5). This is a realistic recognition (not reflected in the Respondents' current submissions) that a power providing for automatic bulk delivery of BCD is a significantly more intrusive step than retention of communications data under DRIPA.

b) Secondly, Mr Beard QC expressly relied both on "*protecting safety and security and in fighting crime*" (p. 6).

c) Thirdly, Mr Beard QC conceded that what was being harmonised (and therefore within the scope of EU law) was any processing by a communications service provider:

> "Article 1(1) of the e-Privacy Directive makes clear that what is being harmonised is the processing of personal data by electronic communications services providers".

d) Fourthly, Mr Beard QC submitted that Article 1(3) of the e-Privacy Directive and Article 4(2) TEU meant that any access to data obtained by the state was outside the scope of EU law, in particular in relation to national security (*"Article 1(3) of the Directive… says matters covered by what were titles 5 and 6 TEU are outside… EU law. So the Directive makes it very clear that there are important limits to its scope… And also that the member states have very carefully set out in Article 4(2) TEU the measures taken for the purposes of national security are the sole responsibility of member states… And of course Article 4(2) is not a derogation therefore not to be construed narrowly"*). Mr Beard QC then submitted that the Court *"could not be laying down mandatory requirements for access on matters outside EU law"* (p. 8). This was a key part of the UK's central submission that whilst *retention* was in scope of EU law, *access* was not: see CJEU judgment at [65] last sentence; UK *Tele2* Written Observations at §§9(iii)-(iv), 20-28 **[JSAuth/1/29]**.

8. The submissions now made to the Tribunal precisely mirror the submissions made by the UK to the CJEU, which were comprehensively rejected. Often, the same phrases used in written and oral submissions to the CJEU have simply been repeated in the Respondents' skeleton (e.g. *"Article 4(2) is not a derogation, and is thus not to be interpreted narrowly"*) [Respondents' Skeleton §19].

9. The CJEU held in *Watson* that EU law was engaged. The analysis offered by the UK about the scope of the Directive was considered and rejected:

> 69. Article 1(3) of that directive excludes from its scope 'activities of the State' in specified fields, including the activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters (see, by analogy, with respect to the first indent of Article 3(2) of Directive 95/46, judgments of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 43, and of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, EU:C:2008:727, paragraph 41).
>
> 70 Article 3 of Directive 2002/58 states that the directive is to apply 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').

Consequently, that directive must be regarded as regulating the activities of the providers of such services.

71 Article 15(1) of Directive 2002/58 states that Member States may adopt, subject to the conditions laid down, 'legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 [of that directive]'. The second sentence of Article 15(1) of that directive identifies, as an example of measures that may thus be adopted by Member States, measures 'providing for the retention of data'.

72 Admittedly, the legislative measures that are referred to in Article 15(1) of Directive 2002/58 concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 51). Moreover, the objectives which, under that provision, such measures must pursue, such as safeguarding national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that directive.

73 However, having regard to the general structure of Directive 2002/58, the factors identified in the preceding paragraph of this judgment do not permit the conclusion that the legislative measures referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.

10. Before the CJEU, the UK emphasised that data retention under DRIPA was less objectionable than a *"wholesale sweep up of data by the investigating authorities… a general database access"* as occurs with the collection of BCD under section 94. The position under section 94 TA 1984 is therefore *a fortiori* the arguments made by Mr Watson and Mr Davis in relation to DRIPA:

a) The Respondents concede that a section 94 direction requires a PECN to carry out processing of communications data within the meaning of the e-Privacy Directive. Retention is one example of processing. See *Watson* at §75: *"The scope of that directive extends, in particular, to a legislative measure, such as that at issue in the main proceedings, that requires such providers to retain traffic and location data, since to*

do so necessarily involves the processing, by those providers, of personal data". Where a commercial provider processes data, that engages EU law, since the terms of permissible processing of communications/traffic and location data *by a PECN* are set by Articles 5, 6, 9 and 15 of the e-Privacy Directive.

b) The CJEU made clear in both *DRI* and in *Watson*, despite the submissions of the UK, that any conduct relying on the derogation in Article 15(1) of the e-Privacy Directive would require a group of basic safeguards against misuse, including prior judicial or independent authorisation, the retention of the data in the EU and provisions for notice to affected persons. None of those safeguards are present in the scheme for collection of BCD under section 94.

Reference to CJEU

11. The Respondents do not suggest that the issues of EU law (including the proper interpretation of Article 4(2) TEU and Article 1(3) of the e-Privacy Directive) are *acte éclairé* in their favour. In circumstances where all the Respondents' arguments were made to the Grand Chamber of the CJEU and rejected in the last year, that position is evidently correct. It is instead *acte éclairé* in the Claimant's favour.

12. As the final national court, from which no appeal or judicial review is presently possible, the Tribunal has a duty to refer to the CJEU any question of EU law that is not *acte clair*; and the continued power to refer questions that that are *acte éclairé* to ask, in effect, if the CJEU stands by its previous judgment. The judgment in *Watson* is clear, including as to the arguments that the UK made in relation to Article 4(2) TEU, but if the Tribunal considers (contrary to the Claimant's primary case) that there is any real scope for doubt as to its interpretation, its duty under Article 267(3) TFEU is to refer further questions to the CJEU to clarify the application of *Watson* in a pure or primarily national security case and ask whether EU law applies to a section 94 direction to a PECN to supply BCD. It may also refer if it wishes, in effect, to ask the CJEU, pursuant to the judicial dialogue occurring between apex courts, to reconsider its judgment.

13. It should also be pointed out that the logic of the Respondents' case is that Article 15(1) of the e-Privacy Directive, insofar as it deals with national security, is *ultra vires* Article 4(2) TEU (and before that *ultra vires* the competences conferred, Article 4(2) being confirmatory rather than freshly constitutive in effect), because the EU has no jurisdiction to require conduct relating to national security to be proportionate. The validity or invalidity of EU secondary legislation such as a Directive is within the exclusive competence of the CJEU, which must be given the opportunity to consider the issue: see *FotoFrost* [1987] ECR 4199. It would not therefore be proper for the Tribunal to accept the Respondents submissions without first making a reference.

14. Finally, the Respondents no longer seek to pursue a *kompetenz-kompetenz* argument at the hearing commencing on 5 June 2017. The Respondents accept the Claimant's submission that such an issue could not arise until after a further reference to the CJEU ("*... the principles of sincere cooperation and mutual respect again dictate that the proper course, in the first instance, is to make reference to the CJEU to enable that Court to clarify the position...*") Only after such a reference would a domestic court have to consider the "*difficult and novel question of some constitutional importance...*" (Respondents' Skeleton §90). It is impossible to see how the 'reverse *Marleasing*' argument the Respondents urge upon the IPT, if it is to occur at all, can happen at any other time: an essential predicate of such unprecedented step is that the national court has decided such step is necessary to avoid a domestic constitutional principle being transgressed; it is a remedial step short of a full blown declaration of the *ultra vires* of a CJEU ruling.

15. All these factors point to the likelihood of a reference. Indeed, it is at present impossible to see how the case could be decided against the Claimant, whether on purported EU grounds or because of domestic constitutional requirements, without such a step first being taken. The Claimant has therefore prepared draft questions to the CJEU in the event that the Tribunal is minded to make such a reference. See the **Annex** to this note.

Sharing

16. Four additional points arise from the Respondents' skeleton:

a) First, the Claimant has not yet seen any reply to the further letter to the Commissioners. It is hoped that any reply received can be provided in advance of the hearing.

b) Secondly, the Third Witness Statement of Ms Graham Wood exhibits documents about the cessation and resumption of intelligence sharing with the US following the terrorist attacks in Manchester. There was repeated disclosure of sensitive information to the US press in breach of the control principle and arrangements for 'Action-on'. If a foreign partner as close and important as the US is unwilling or unable to respect the confidence attached to materials in an ongoing terrorist investigation, it is doubtful if proper control can be exercised over a whole dataset or access to it.

c) Thirdly, the Respondents' position is that equivalence of standards and safeguards is not required when MI5 and MI6 share entire datasets of information, including bulk data about large numbers of people of no intelligence interest. Safeguards are only applied *"insofar as considered appropriate"* [Respondents' Skeleton §115.5]. But that leaves open the prospect that no safeguards, or substantially lesser safeguards, might be *"considered appropriate"* by an official, without even obtaining approval from the Secretary of State as would be required for intercept material. The Respondents have not dealt with these points in its skeleton argument.

d) Finally, the Respondents have failed to address the Claimant's submissions on circumvention of the law through sharing of bulk data in §91-95 of the Claimant's skeleton argument. The Respondents suggest that this cannot be dealt with in OPEN. This is incorrect. The questions are issues of principle, to be determined on the assumption that such sharing might take place. These points have been pleaded and ready for determination for many months. The reality, uncomfortable as it is for the legality of these arrangements, is that highly intrusive material that can only lawfully be obtained for strict national security

purposes, is, upon receipt by the Respondents, being widely "repurposed" to support a variety of other law enforcement purposes, such as criminal investigations into tax evasion.

THOMAS DE LA MARE QC

BEN JAFFEY QC

DANIEL CASHMAN

Blackstone Chambers

BHATT MURPHY

2 June 2017

ANNEX

Bulk Communications Data

A national provision requires a public electronic communications network ("the PECN") to comply with a direction made by a senior politician with responsibility for national security in the interests of national security ("the Direction"). The Direction requires the PECN to extract and provide communications data obtained and used by the PECN in the course of providing its telecommunications service to that state's security and intelligence services in bulk.

1. Is such Direction outside the scope of EU law, by virtue of Article 4(2) TEU and Article 1(3) of the e-Privacy Directive, because such Direction is and can only be made for reasons of national security?

2. If the answer to question 1 is "no", does Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11, 47 and Article 52(1) of the Charter of Fundamental Rights preclude such a Direction where it (and, as applicable, the national regime underpinning the Direction):

    a. requires the PECN to provide bulk communications data;

    b. fails to subject either the making of any Direction or any form of use of communications data supplied pursuant to the Direction to a requirement of prior judicial or independent authorisation;

    c. does not require the data subjects to be notified of the fact that their communications data have been processed other than for the provision of telecommunications services;

    d. imposes constraints on sharing of communications data only by means of internal guidance;

    e. imposes no prohibition upon the communications data so taken being transferred out of the EU.

3. If the answer to question 1 is "yes" or the answer of any of questions 2a. to e. is "no" because of the national security basis of the direction, is the matter brought back in the scope of EU law or does the answer to questions 2.a. to e. change if the bulk communications data are thereafter either (a) used for purposes connected with the prevention or detection of serious crime; and/or (b) shared with other agencies for the purposes of prevention and detection of serious crime?

Bulk Personal Datasets

4. In the case of a national provision that requires (for instance, pursuant to a direction or requirement imposed as part of the prior or continued authorisation of that person to provide services) a party carrying out commercial activity engaging EU law (such as the operation of a port, airport or transport provider) to provide personal data in bulk to a state's security and intelligence services for the purposes of national security and/or the prevention and detection of serious crime, is such a provision outside the scope of EU law, by virtue of Article 4(2) TEU and Article 3(2) of the Data Protection Directive?

5. If the answer to question 4 is "no", does EU law and Articles 7, 8 and 11, 47 and Article 52(1) of the Charter of Fundamental Rights preclude national legislation (or Directions or requirements made under it) which:

   a. requires the PECN to provide personal data in bulk;

   b. fail to subject either the making of any requirement or any form of use of personal data to a requirement of prior judicial or independent authorisation;

   c. does not require the data subjects to be notified of the fact that their data have been processed;

   d. imposes constraints on sharing of personal data only by means of internal guidance;

   e. imposes no prohibition upon the personal data so taken being transferred out of the EU.

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

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

CLAIMANT'S REPLY NOTE

Privacy International
62 Britton Street
London
EC1M 5UY

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